

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-275203

(43)Date of publication of application : 13.10.1998

(51)Int.Cl.

G06K 17/00
G06T 7/00
G06K 19/10
G06K 19/06
H04L 9/32

(21)Application number : 09-227979

(71)Applicant : NEC CORP

(22)Date of filing : 25.08.1997

(72)Inventor : TAKAI KAZUTO
FUJIWARA SHIRO

(30)Priority

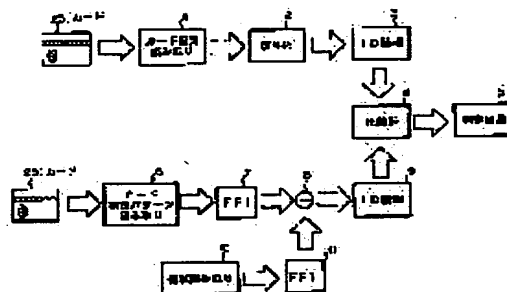
Priority number : 08317545	Priority date : 28.11.1996	Priority country : JP
08357504	27.12.1996	
09 20602	03.02.1997	JP
		JP

(54) CARD TYPE RECORDING MEDIUM, METHOD AND DEVICE FOR ITS AUTHENTICATION, PREPARING SYSTEM, CIPHERING SYSTEM, ITS DECIPHERING DEVICE AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To improve security by providing information to input in a magnetic card for both of magnetic data and the pattern of the card to prevent a third party from easily duplicate the card and to discriminate when it is duplicated.

SOLUTION: Written fingerprint pattern written in the card 25 is read by a card image reader 6 and the image is Fourier-transformed at a high speed by FFT 7. On the other hand, the fingerprint pattern of the present owner himself is read by a fingerprint pattern reader 10 and the data is Fourier-transformed at a high speed by FFT 11. A subtractor 8 subtracts the output of FFT 11 from the output of FFT 7 to extract ID information specifying a user. In addition the magnetic data of the card 25 is read by a magnetic reader 1 and a decoding processor 2 deciphers the code to extract ID information 3. Then ID information 9 extracted from the card 25 and ID information 3 extracted from magnetic data are compared by a comparator 4 and a judging circuit 5 judges illegally duplicated information from the result.



LEGAL STATUS

[Date of request for examination]	25.08.1997
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3075221
[Date of registration]	09.06.2000
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of]	

rejection]

[Date of extinction of right]

Copyright (C), 1998,2000 Japanese Patent Office

* NOTICES *

The Japanese Patent Office is not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.*** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] In the card type record medium containing the picture image field where the data area on which the data containing an owner's ID information were recorded, and image data are recorded in the aforementioned picture image field Transform processing to the data of a frequency domain is performed to the 1st image data which specifies the owner itself. The card type record medium characterized by recording the 2nd image data generated by adding the aforementioned ID information to the data of the frequency domain after this conversion, and carrying out the inverse transformation of this added data to a picture signal.

[Claim 2] ID information on the aforementioned data area is a card type record medium according to claim 1 characterized by what is enciphered and recorded.

[Claim 3] The 1st aforementioned image data is a card type record medium according to claim 1 or 2 characterized by being an owner's fingerprint picture image or photograph-of-his-face picture image.

[Claim 4] Transform processing to the data of the aforementioned frequency domain is the claim 1 characterized by being Fourier transformation, or a card type record medium given in 2 and 3.

[Claim 5] Transform processing to the data of the aforementioned frequency domain is the claim 1 characterized by being the discrete cosine conversion given to each of the block which divides the 1st aforementioned image data into plurality, and is acquired, or a card type record medium given in 2 and 3.

[Claim 6] It is a card type record medium containing the picture image field where the data area on which the data containing an owner's ID information were recorded, and image data are recorded. in the aforementioned picture image field Transform processing to the data of a frequency domain is performed to the 1st image data which specifies the owner itself. It is the card type record-medium authentication technique that the 2nd image data generated by adding the aforementioned ID information to the data of the frequency domain after this conversion, and carrying out the inverse transformation of this added data to a picture signal is recorded. The 1st step which reads the data of the aforementioned picture image field while the aforementioned ID information is restored from the aforementioned card type record medium, The 2nd step which performs transform processing to the data of a frequency domain to the data of the aforementioned picture image field, and generates the 1st resolution picture data, The 3rd step which acquires the same image data as the 1st aforementioned image data from other than the aforementioned record medium, performs transform processing to the data of the aforementioned frequency domain to the acquired image data, and obtains the 2nd resolution picture data, the difference which subtracted and obtained the resolution picture data of the above 2nd from the resolution picture data of the above 1st — the card type record-medium authentication technique characterized by consisting of the 4th step which compares ID information restored from data and the aforementioned card type record medium, and judges the justification of the aforementioned storage

[Claim 7] Transform processing to the data of the aforementioned frequency domain is the card type record-medium authentication technique according to claim 6 characterized by being Fourier transformation.

[Claim 8] Transform processing to the data of the aforementioned frequency domain is the card type record-medium authentication technique according to claim 6 characterized by being the discrete cosine conversion given to each of the block which divides the 1st aforementioned image data into plurality, and is acquired.

[Claim 9] the above with which the 4th aforementioned step was obtained for every aforementioned block — the difference — the claim 6 which compares ID information restored from data and the aforementioned card type record medium, and is characterized by making the aforementioned judgment by the majority of a comparison result, or the card type record-medium authentication technique given in 7 and 8

[Claim 10] It is a card type record medium containing the picture image field where the data area on which the data containing an owner's ID information were recorded, and image data are recorded. in the aforementioned picture image field Transform processing to the data of a frequency domain is performed to the 1st image data which specifies the owner itself. In the card type record-medium authentication equipment with which the 2nd image data generated by adding the aforementioned ID information to the data of the frequency domain after this conversion, and carrying out the inverse transformation of this added data to a picture signal is recorded ID information reading machine which restores the aforementioned ID information from the aforementioned card type record medium, The picture image reading machine which reads the data of the aforementioned picture image field, and the transform-processing section which performs transform processing to the data of a frequency domain to the data of the aforementioned picture image field, and generates the 1st resolution picture data, The 2nd picture image reading machine which reads the same image data as the 1st aforementioned image data in other than the aforementioned record medium, The 2nd transform-processing section which performs transform processing to the data of the aforementioned frequency domain to the acquired image data, and obtains the 2nd resolution picture data, the resolution picture data of the resolution picture data of the above 1st to the above 2nd — subtracting — the difference — with the subtractor which obtains data the above — the difference — the judgment circuit which compares ID information restored from data and the aforementioned card type record medium, and judges the justification of the aforementioned card type storage — ** — since — the card type record-medium authentication equipment characterized by becoming

[Claim 11] In the card type record-medium cipher system containing an encryption means to encipher ID information recorded on a magnetic card, and a magnetic information creation means to make a magnetic information enciphered ID information and to record on the aforementioned magnetic card A frequency-domain conversion means to change the subject-copy pattern of the pattern of the aforementioned magnetic card into the information on a frequency domain, An addition means to change ID information recorded on the aforementioned magnetic card into the conversion information distributed over the frequency

domain, and to add the aforementioned conversion information and the information generated by conversion by the aforementioned frequency-domain conversion means, A frequency-domain inverse-transformation means to return the information on the frequency domain generated by the addition by the aforementioned addition means to a two-dimensional picture image pattern. The card type record-medium cipher system characterized by having a picture image pattern printing means to print to the concerned magnetic card so that the picture image pattern generated by the aforementioned frequency-domain inverse-transformation means may be used as a pattern of the aforementioned magnetic card.

[Claim 12] The card type record-medium cipher system according to claim 11 characterized by having an addition means to make it similar to distribution **** of the subject-copy image frequency spectrum which is an information on the frequency domain generated by conversion by the aforementioned frequency-domain conversion means, to generate ID information frequency spectrum, and to add the concerned subject-copy image frequency spectrum and the concerned ID information frequency *****.

[Claim 13] The card type record-medium cipher system according to claim 11 or 12 characterized by for the aforementioned frequency-domain conversion means performing FFT, and a frequency-domain inverse-transformation means performing reverse FFT.

[Claim 14] The card type record-medium cipher system according to claim 11 or 12 characterized by for the aforementioned frequency-domain conversion means performing DCT, and a frequency-domain inverse-transformation means performing reverse DCT.

[Claim 15] In the card type record-medium decoder of the record medium which stenciled the picture image pattern containing enciphered ID information and ID information The magnetic read station which reads in the magnetic stripe of the aforementioned record medium ID information by which encryption was carried out [aforementioned], A frequency-domain conversion means to change the subject-copy pattern of the pattern of a magnetic card into the information on a frequency domain by the aforementioned magnetic head, A reverse encryption means to reverse-encipher ID information by which encryption was carried out [aforementioned], and to output ID information, A picture image reading means to read the aforementioned picture image pattern, and a frequency-domain conversion means to change the aforementioned picture image pattern into a frequency domain, the subtractor which deducts the data which changed the aforementioned ID information into the frequency domain from the data of the aforementioned frequency domain, and a frequency-domain inverse-transformation means to return the information on the frequency domain generated by subtraction by the aforementioned subtractor to a two-dimensional picture image pattern — since — the becoming card type record-medium decoder

[Claim 16] The card type record medium characterized by recording further the image data generated by carrying out the inverse transformation of the aforementioned spatial-frequency data with which the aforementioned identification data were embedded to a time data after embedding the identification data which are the card type record medium with which the specific data which specify an owner were written in, and were generated based on the aforementioned specific data in the spatial-frequency data of a photograph.

[Claim 17] It is the card type record medium according to claim 16 which the aforementioned spatial-frequency data are the photograph picture image by which dispersed cosine conversion was carried out, and is characterized by the aforementioned inverse transformation being reverse dispersed cosine conversion.

[Claim 18] the component to which, as for the aforementioned spatial-frequency data with which the aforementioned identification data were embedded, each component of the spatial-frequency data of the aforementioned photograph data and the aforementioned identification data correspond — a multiplication — carrying out — this multiplication value — constant twice — the card type record medium according to claim 16 or 17 characterized by being data created by adding the value carried out to the component to which the spatial-frequency data of the aforementioned photograph data correspond

[Claim 19] The aforementioned specific data are a card type record medium given in the claim 16 characterized by being written in the magnetic-recording section, or any 1 term of 18.

[Claim 20] The card type record medium characterized by using a card type record medium given in the claim 16 or any 1 term of 18 for an identification card or a credit card.

[Claim 21] A means to generate identification data based on the specific data which specify an owner, The multiplication of a means to change into spatial-frequency data the photograph which should be stuck, and each component of the aforementioned spatial-frequency data and the component to which the aforementioned identification data correspond is carried out. this multiplication value — constant twice — with a means to add the value carried out to the component to which the spatial-frequency data of the aforementioned photograph data correspond, to carry out the inverse transformation of this added spatial-frequency data, and to change into image data The card type record-medium creation system characterized by having the means which writes the aforementioned image data and the aforementioned specific data in a card type record medium.

[Claim 22] It is the card type record-medium creation system according to claim 21 which the aforementioned conversion is dispersed cosine conversion and is characterized by the aforementioned inverse transformation being reverse dispersed cosine conversion.

[Claim 23] After embedding the identification data generated based on the specific data which specify an owner in the spatial-frequency data of a photograph It is the card type record-medium authentication equipment recorded with the aforementioned specific data in the image data generated by carrying out the inverse transformation of the aforementioned spatial-frequency data with which the aforementioned identification data were embedded to a time data. A means to generate the aforementioned identification data based on the aforementioned specific data, and a conversion means to change the aforementioned image data into the aforementioned spatial-frequency data, Card type record-medium authentication equipment equipped with a means to perform the correlation operation of the output of the aforementioned conversion means, and the aforementioned identification data, and to judge the truth or falsehood of a card type record medium based on this correlation result of an operation.

[Claim 24] The step which generates identification data based on the specific data which are the record medium which stored the program for operating a card type record-medium creation system in a computer, and specify an owner, The step which changes into spatial-frequency data the photograph picture image which should be stuck, The multiplication of each component of the aforementioned spatial-frequency data and the component to which the aforementioned identification data correspond is carried out. this multiplication value — constant twice — with the step which adds the value carried out to the component to which the spatial-frequency data of the aforementioned photograph picture image correspond, carries out the inverse transformation of this added spatial-frequency data, and is changed into image data The record medium characterized by storing the program containing the step which writes the aforementioned image data and the aforementioned specific data in a card type record medium.

[Claim 25] It is the record medium characterized by for the aforementioned conversion being dispersed cosine conversion and storing the program for operating in a computer the card type record-medium creation system according to claim 24 characterized by the aforementioned inverse transformation being reverse dispersed cosine conversion.

[Claim 26] After embedding the identification data generated based on the specific data which specify an owner in the spatial-frequency data of a photograph The image data generated by carrying out the inverse transformation of the aforementioned spatial-frequency data with which the aforementioned identification data were embedded to a time data The step which is the record medium which stored the program for operating in a computer the check system of the card type record medium recorded with the aforementioned specific data, and generates the aforementioned identification data based on the aforementioned specific data, The record medium characterized by storing the program containing the step which changes the aforementioned image data into spatial-frequency data, and the step which performs the correlation operation of this conversion result and the aforementioned identification data, and judges the truth or falsehood of a card type record medium based on this correlation result of an operation.

[Claim 27] In the card type record medium containing the picture image field where the data area on which the data containing ID information peculiar to an owner were recorded, and image data are recorded in the aforementioned picture image field Transform processing to the data of a frequency domain is performed to the 1st image data which specifies the owner itself. The card type record medium characterized by recording the 2nd image data generated by adding the data which changed the aforementioned ID information into the data of the frequency domain after this conversion at the frequency domain, and carrying out the inverse transformation of this added data to a picture signal.

[Claim 28] ID information on the aforementioned data area is a card type record medium according to claim 27 characterized by what is enciphered and recorded.

[Claim 29] The 1st aforementioned image data is a card type record medium according to claim 27 or 28 characterized by being an owner's fingerprint picture image or photograph-of-his-face picture image.

[Translation done.]

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平10-275203

(43)公開日 平成10年(1998)10月13日

(51)Int.Cl.⁶

識別記号

F I

G 0 6 K 17/00

G 0 6 K 17/00

T

G 0 6 T 7/00

G 0 6 F 15/62

4 6 0

G 0 6 K 19/10

G 0 6 K 19/00

R

19/06

B

審査請求 有 請求項の数29 O L (全 20 頁) 最終頁に続く

(21)出願番号 特願平9-227979

(22)出願日 平成9年(1997)8月25日

(31)優先権主張番号 特願平8-317545

(32)優先日 平8(1996)11月28日

(33)優先権主張国 日本 (J P)

(31)優先権主張番号 特願平8-357504

(32)優先日 平8(1996)12月27日

(33)優先権主張国 日本 (J P)

(31)優先権主張番号 特願平9-20602

(32)優先日 平9(1997)2月3日

(33)優先権主張国 日本 (J P)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 高井 和人

東京都港区芝五丁目7番1号 日本電気株式会社内

(72)発明者 藤原 司郎

東京都港区芝五丁目7番1号 日本電気株式会社内

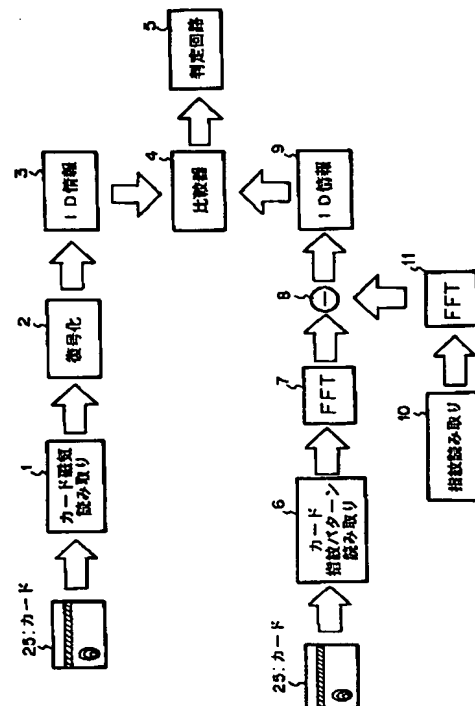
(74)代理人 弁理士 山下 稔平

(54)【発明の名称】 カード型記録媒体及びその認証方法及び認証装置、作成システム、暗号化方式、その解読器と記録媒体

(57)【要約】

【課題】 カード型記録媒体の偽造及び不正使用の困難なセキュリティを向上したカード型記録媒体を提供する。

【解決手段】 予め磁気カードの上に磁気データと同一の情報を、本人の指紋パターンをフーリエ変換 (F F T)、又はD C T変換した周波数スペクトラムパターンに重ねて、そのパターンを逆F F T変換して磁気カードに印刷しておく。また、磁気カードの模様の原画パターンを周波数ドメインの情報にF F T又はD C T変換し、当該磁気カードのI D情報を周波数ドメインに分布させた情報を生成し、当該生成情報と変換された情報とを加算し、加算手段による加算によって生成された周波数ドメインの情報を2次元の画像パターンに戻し、生成された画像パターンを当該磁気カードの模様として使うように当該磁気カードに印刷する。また、身分証明書についても、顔写真に識別コードを埋め込み、正規の所有者と顔写真の所有者とが同一か否かを判定する。



【特許請求の範囲】

【請求項1】 所有者のID情報を含むデータが記録されたデータ領域と画像データが記録される画像領域とを含むカード型記録媒体において、

前記画像領域には、所有者自身を特定する第1の画像データに周波数領域のデータへの変換処理を施し、この変換後の周波数領域のデータに前記ID情報を加算し、この加算されたデータを画像信号に逆変換することにより生成された第2の画像データが記録されていることを特徴とするカード型記録媒体。

【請求項2】 前記データ領域のID情報は、暗号化されて記録されていることを特徴とする請求項1に記載のカード型記録媒体。

【請求項3】 前記第1の画像データは、所有者の指紋画像又は顔写真画像であることを特徴とする請求項1又は2に記載のカード型記録媒体。

【請求項4】 前記周波数領域のデータへの変換処理は、フーリエ変換であることを特徴とする請求項1又は2、3に記載のカード型記録媒体。

【請求項5】 前記周波数領域のデータへの変換処理は、前記第1の画像データを複数個に分割して得られるブロックの各々に施されるディスクリットコサイン変換であることを特徴とする請求項1又は2、3に記載のカード型記録媒体。

【請求項6】 所有者のID情報を含むデータが記録されたデータ領域と画像データが記録される画像領域とを含むカード型記録媒体であり、前記画像領域には、所有者自身を特定する第1の画像データに周波数領域のデータへの変換処理を施し、この変換後の周波数領域のデータに前記ID情報を加算し、この加算されたデータを画像信号に逆変換することにより生成された第2の画像データが記録されているカード型記録媒体認証方法であり、

前記カード型記録媒体から前記ID情報を復元するとともに、前記画像領域のデータを読み取る第1のステップと、

前記画像領域のデータに周波数領域のデータへの変換処理を施して第1の変換画像データを生成する第2のステップと、

前記第1の画像データと同じ画像データを前記記録媒体以外から取得し、取得した画像データに前記周波数領域のデータへの変換処理を施して第2の変換画像データを取得する第3のステップと、

前記第1の変換画像データから前記第2の変換画像データを減算して得た差分データと前記カード型記録媒体から復元されたID情報とを比較し、前記記憶媒体の正当性を判断する第4のステップ、とからなることを特徴とするカード型記録媒体認証方法。

【請求項7】 前記周波数領域のデータへの変換処理は、フーリエ変換であることを特徴とする請求項6に記載

のカード型記録媒体認証方法。

【請求項8】 前記周波数領域のデータへの変換処理は、前記第1の画像データを複数個に分割して得られるブロックの各々に施されるディスクリットコサイン変換であることを特徴とする請求項6に記載のカード型記録媒体認証方法。

【請求項9】 前記第4のステップは、前記ブロック毎に得られた前記差分データと前記カード型記録媒体から復元されたID情報とを比較し、比較結果の多数決により、前記判断を行うことを特徴とする請求項6又は7、8に記載のカード型記録媒体認証方法。

【請求項10】 所有者のID情報を含むデータが記録されたデータ領域と画像データが記録される画像領域とを含むカード型記録媒体であり、前記画像領域には、所有者自身を特定する第1の画像データに周波数領域のデータへの変換処理を施し、この変換後の周波数領域のデータに前記ID情報を加算し、この加算されたデータを画像信号に逆変換することにより生成された第2の画像データが記録されているカード型記録媒体認証装置において、

前記カード型記録媒体から前記ID情報を復元するID情報読取器と、

前記画像領域のデータを読み取る画像読取器と、

前記画像領域のデータに周波数領域のデータへの変換処理を施して第1の変換画像データを生成する変換処理部と、

前記第1の画像データと同じ画像データを前記記録媒体以外から読取る第2の画像読取器と、

取得した画像データに前記周波数領域のデータへの変換処理を施して第2の変換画像データを取得する第2の変換処理部と、

前記第1の変換画像データから前記第2の変換画像データを減算して差分データを得る減算器と、

前記差分データと前記カード型記録媒体から復元されたID情報とを比較して前記カード型記憶媒体の正当性を判断する判定回路と、とからなることを特徴とするカード型記録媒体認証装置。

【請求項11】 磁気カードに記録するID情報を暗号化する暗号化手段と、暗号化されたID情報を磁気情報として前記磁気カードに記録する磁気情報作成手段とを含むカード型記録媒体暗号化方式において、

前記磁気カードの模様を原画パターンを周波数ドメインの情報に変換する周波数ドメイン変換手段と、

前記磁気カードに記録するID情報を周波数ドメインに分布させた変換情報に変換し、前記変換情報と前記周波数ドメイン変換手段による変換によって生成された情報とを加算する加算手段と、

前記加算手段による加算によって生成された周波数ドメインの情報を2次元の画像パターンに戻す周波数ドメイン逆変換手段と、

前記周波数ドメイン逆変換手段によって生成された画像パターンを前記磁気カードの模様として使うように当該磁気カードに印刷する画像パターン印刷手段とを有することを特徴とするカード型記録媒体暗号化方式。

【請求項 12】 前記周波数ドメイン変換手段による変換によって生成された周波数ドメインの情報である原画像周波数スペクトラムの分布状態に類似させて ID 情報周波数スペクトラムを生成して当該原画像周波数スペクトラムと当該 ID 情報周波数スペクトラムとを加算する加算手段とを有することを特徴とする請求項 11 に記載のカード型記録媒体暗号化方式。

【請求項 13】 前記周波数ドメイン変換手段が FFT を行い、周波数ドメイン逆変換手段が逆 FFT を行うことを特徴とする請求項 11 又は 12 に記載のカード型記録媒体暗号化方式。

【請求項 14】 前記周波数ドメイン変換手段が DCT を行い、周波数ドメイン逆変換手段が逆 DCT を行うことを特徴とする請求項 11 又は 12 に記載のカード型記録媒体暗号化方式。

【請求項 15】 暗号化された ID 情報と、ID 情報を含む画像パターンを刷り込んだ記録媒体のカード型記録媒体解読器において、

前記記録媒体の磁気ストライプから前記暗号化された ID 情報を読み取る磁気読取部と、

前記磁気ヘッドで磁気カードの模様の原画像パターンを周波数ドメインの情報に変換する周波数ドメイン変換手段と、

前記暗号化された ID 情報を逆暗号化して ID 情報を出力する逆暗号化手段と、

前記画像パターンを読み取る画像読取手段と、

前記画像パターンを周波数ドメインに変換する周波数ドメイン変換手段と、

前記周波数ドメインのデータから前記 ID 情報を周波数ドメインに変換したデータを差し引く減算器と、前記減算器による減算によって生成された周波数ドメインの情報を 2 次元の画像パターンに戻す周波数ドメイン逆変換手段と、からなるカード型記録媒体解読器。

【請求項 16】 所有者を特定する特定データが書き込まれたカード型記録媒体であって、

前記特定データに基づいて生成された識別データを、写真の空間周波数データ内に埋め込んだ後に、前記識別データが埋め込まれた前記空間周波数データを時間データに逆変換することにより生成された画像データを更に記録していることを特徴とするカード型記録媒体。

【請求項 17】 前記空間周波数データは、離散的コサイン変換された写真画像であり、前記逆変換は、逆離散的コサイン変換であることを特徴とする請求項 16 に記載のカード型記録媒体。

【請求項 18】 前記識別データが埋め込まれた前記空間周波数データは、前記写真データの空間周波数データ

の各成分と前記識別データの対応する成分とを乗算し、この乗算値を定数倍した値を、前記写真データの空間周波数データの対応する成分に加算することにより作成されたデータであることを特徴とする請求項 16 又は 17 に記載のカード型記録媒体。

【請求項 19】 前記特定データは、磁気記録部に書き込まれていることを特徴とする請求項 16 乃至 18 のいずれか 1 項に記載のカード型記録媒体。

【請求項 20】 請求項 16 乃至 18 のいずれか 1 項に記載のカード型記録媒体を身分証明書又はクレジットカードに用いることを特徴とするカード型記録媒体。

【請求項 21】 所有者を特定する特定データに基づいて識別データを生成する手段と、

貼付されるべき写真を、空間周波数データに変換する手段と、

前記空間周波数データの各成分と前記識別データの対応する成分とを乗算し、この乗算値を定数倍した値を前記写真データの空間周波数データの対応する成分に加算し、この加算された空間周波数データを逆変換して画像データに変換する手段と、

前記画像データと前記特定データとをカード型記録媒体に書き込む手段とを備えたことを特徴とするカード型記録媒体作成システム。

【請求項 22】 前記変換は離散的コサイン変換であり、前記逆変換は逆離散的コサイン変換であることを特徴とする請求項 21 に記載のカード型記録媒体作成システム。

【請求項 23】 所有者を特定する特定データに基づいて生成された識別データを、写真の空間周波数データ内に埋め込んだ後に、前記識別データが埋め込まれた前記空間周波数データを時間データに逆変換することにより生成された画像データを前記特定データとともに記録されたカード型記録媒体認証装置であって、

前記特定データに基づいて前記識別データを生成する手段と、

前記画像データを前記空間周波数データに変換する変換手段と、

前記変換手段の出力と前記識別データとの相関演算を行い、この相関演算結果に基づいてカード型記録媒体の真贋を判定する手段とを備えたカード型記録媒体認証装置。

【請求項 24】 カード型記録媒体作成システムを電子計算機で動作させるためのプログラムを格納した記録媒体であり、

所有者を特定する特定データに基づいて識別データを生成するステップと、

貼付されるべき写真画像を、空間周波数データに変換するステップと、

前記空間周波数データの各成分と前記識別データの対応する成分とを乗算し、この乗算値を定数倍した値を前記

写真画像の空間周波数データの対応する成分に加算し、この加算された空間周波数データを逆変換して画像データに変換するステップと、

前記画像データと前記特定データとをカード型記録媒体に書き込むステップとを含むプログラムを格納したことを特徴とする記録媒体。

【請求項 25】 前記変換は離散的コサイン変換であり、前記逆変換は逆離散的コサイン変換であることを特徴とする請求項 24 に記載のカード型記録媒体作成システムを電子計算機で動作させるためのプログラムを格納したことを特徴とする記録媒体。

【請求項 26】 所有者を特定する特定データに基づいて生成された識別データを、写真の空間周波数データ内に埋め込んだ後に、前記識別データが埋め込まれた前記空間周波数データを時間データに逆変換することにより生成された画像データが、前記特定データとともに記録されたカード型記録媒体の検査システムを電子計算機で動作させるためのプログラムを格納した記録媒体であり、前記特定データに基づいて前記識別データを生成するステップと、前記画像データを空間周波数データに変換するステップと、

この変換結果と前記識別データとの相関演算を行い、この相関演算結果に基づいてカード型記録媒体の真贋を判定するステップとを含むプログラムを格納したことを特徴とする記録媒体。

【請求項 27】 所有者固有の ID 情報を含むデータが記録されたデータ領域と画像データが記録される画像領域とを含むカード型記録媒体において、前記画像領域には、所有者自体を特定する第 1 の画像データに周波数領域のデータへの変換処理を施し、この変換後の周波数領域のデータに前記 ID 情報を周波数領域に変換したデータを加算し、この加算されたデータを画像信号に逆変換することにより生成された第 2 の画像データが記録されていることを特徴とするカード型記録媒体。

【請求項 28】 前記データ領域の ID 情報は、暗号化されて記録されていることを特徴とする請求項 27 に記載のカード型記録媒体。

【請求項 29】 前記第 1 の画像データは、所有者の指紋画像又は顔写真画像であることを特徴とする請求項 27 又は 28 に記載のカード型記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、クレジットカードやキャッシュカード、身分証明書等の磁気カードを含むカード型記録媒体に関し、特にそのカード型記録媒体の正当性を検証する認証方法、磁気カードに記録される ID (Identification) 情報の暗号化を行うカード型記録

媒体暗号化方式、文字化された個人データと共に本人の顔写真が記録されたカード型記録媒体、さらに当該カード型記録媒体の作成方法や解読方法をコンピュータのプログラムとして記録した記録媒体に関する。

【0002】

【従来の技術】従来、クレジットカードやキャッシュカードの様な磁気カードの正当な所有者を検証する技術や磁気カード ID 情報暗号化方式としては、たとえば特開昭 64-76270 号公報に示されるように、クレジットカードやキャッシュカードとして使用される磁気カードにおいて、当該磁気カードの所有者を確認する際のセキュリティを向上させるために、当該磁気カードに記録しておきたい磁気情報としての ID 情報と引き出し金額等の価値情報等の暗号化を行い、また磁気カードに暗号化された所有者の ID 情報が記憶され、磁気カードから ID 情報を復号し、所有者が別途入力する ID 情報と比較することにより、そのカードの正当な所有者であることを検証している（以下、「第 1 の従来技術」）。

【0003】図 20 は、従来の磁気カード ID 情報暗号化方式の一例の構成を示すブロック図である。以下に、図 20 を参照して、従来の磁気カード ID 情報暗号化方式の動作を説明する。暗号化手段 72 は、磁気カードの ID 情報 71 の磁気情報を読み込んだだけでは容易に当該 ID 情報のデータの分析ができないように、当該 ID 情報 71 の暗号化を行う（暗号化の様態としては様々なものが存在する）。磁気情報作成手段 73 は、暗号化手段 72 によって生成された磁気情報（暗号化された ID 情報）を磁気カード上の磁気記録部分（磁気ストライプ等）に記録する。

【0004】また、特開平 06-135187 号公報は、カード本来が記憶している磁気データ以外に、所有者の顔写真をカードに印刷され、また写真情報を暗号化したデータも印刷された磁気カードを開示している。この公報記載の技術では、カードの保有者の外観情報を表示した画像領域と、該画像情報を所定のロジックに基づき変換した暗号情報を表示したスクランブル領域とを備え、その暗号化した写真情報を逆ロジックで復号し、顔写真の画像情報との同一性を照合され、カードの正当性を機械的に判別している（以下、「第 2 の従来技術」）。

【0005】更に近年、写真付きの身分証明書が普及している。パスポート、民間企業の社員証、各種免許証などがそうである。またクレジットカードにも写真の貼られたものが普及しつつあり、これらを総称して「身分証明書」と称する。特に公的機関が発行したもので、写真が貼られているものは身分の確認に利用されている。しかし、これらの身分証明書は偽造されることがある。現実には、写真を刷り込み印刷することで、偽造しにくくしたはずの現在の小型のパスポートでも、すでに写真のみを貼りかえた偽造パスポートが出ている。しかも、この

偽造パスポートは非常に精巧にできており、偽造と見破るのがかなり困難なものになっている。

【0006】この偽造パスポートを含め偽造身分証明書ができる理由は、次の2つがあげられる。(1)写真を貼りがえることができる。(2)写真と身分証明書に記載されている項目とに関連がまったくない。いいかえれば、写真のみ貼りがえて他の記載事項を変更しなくても、その身分証明書は、一見しただけでは真正のものか、偽造のものかを判別できない。

【0007】これを防ぐには、(a)偽造行為そのものが困難のように身分証明書を作成する方法、(b)偽造されたとしても、その身分証明書が偽造であることを判別することで、偽造身分証明書の使用を防止する方法が必要となる。

【0008】ここで、(a)の方法の一例が、特開平3-193495号公報に示されている(以下、「第3の従来技術」)。この公報では、顔写真情報や属性情報、レイアウト情報等を取り込んだ画像処理装置を用いたIDカード発行システムにおいて、前記情報に加えて偽造防止情報をも画像処理してイメージパターンとし、複雑なパタンを写真の上に重ね合わせ、その重ね合わせた写真を身分証明書に印刷する方法をとっている。この方法で写真に重ね合わせるパターンを複雑にすることで、偽造を防止する効果をねらっている。

【0009】また、(b)の方法としては、特開平3-185585号公報の第5の実施例に示されたものがある(以下、「第4の従来技術」)。この例では、身分証明書に記載されているデータに基づいて、真正身分証明書か、偽造身分証明書かを判別する為の識別データを作成し、それを身分証明書の写真部分に重ね合わせて印刷する方法をとっている。この方法であれば、身分証明書の記載事項と写真に重ね合わされている識別データとを照合できるため、写真を貼りがえられたとしても、偽造を見抜くことができる。

【0010】また、この特開平3-185585号公報には、写真の中にこの識別データを埋め込んでしまう方法も記載されている。記載事項から計算によって識別データを求め、これを写真の一部分に埋め込むことにより実現している。

【0011】別の観点からすると、身分証明書に印刷されている写真が正規のものであることが判別されれば、偽造であることを判別することができる。そこで、画像を周波数変換し、周波数スペクトラムに電子透かし(Digital Watermark)データを埋め込む方法が提案されている(日経エレクトロニクス 1996. 4. 22 (No. 660) 13ページ, 同誌1997. 2. 24 (No. 683) 99-124ページ)(以下、「第5の従来技術」)。この方法においては、オリジナル作品をDCTや高速フーリエ変換で周波数変換し、周波数スペクトラムにユーザ毎に固有の乱数のID情報を加え

てスペクトラム拡散する。このID情報を含む周波数スペクトラムを逆周波数変換して、ID情報を隠し持つ周波数スペクトラムとオリジナル作品の周波数スペクトラムとの差分を取ればID情報が生成されるので、このID情報を正規のID情報とを比較すれば、正規に購入したオリジナル作品であるのか否かを判断することができる。このID情報を低域周波数成分の周波数スペクトラムとして、周波数成分に電子透かしデータを埋め込むので、圧縮処理やフィルタリング等の画像処理に対しても電子透かしデータが失われることはない。さらに、電子透かしデータとして正規分布に従う乱数を採用することで、電子透かしデータ同士の干渉を防ぎ、画質に大きな影響を及ぼすことなく電子透かしデータを破壊することを困難にしている。

【0012】この電子透かしデータの埋め込み方法は、次のとおりである。まず、元の画像を離散コサイン(DCT)変換などを用いて周波数成分に変換し、周波数領域で高い値を示すデータを n 個選び、 $f(1), f(2), \dots, f(n)$ とする。次に電子透かしデータ $w(1), w(2), \dots, w(n)$ を平均0分散1である正規分布より選び、 $F(i) = f(i) + \alpha |f(i)| * w(i)$ を各周波数成分 i について計算する。ここで α はスケールリング要素である。最後に $f(i)$ の変わりに $F(i)$ を置き換えた周波数成分に逆離散コサイン変換を施し、電子透かしデータが埋め込まれた画像を得る。

【0013】電子透かしデータの検出は以下の方法で行う。この検出方法においては、元の画像、及び電子透かしデータ候補 $w(i)$ (但し $i=1, 2, \dots, n$)が既知でなければならない。

【0014】まず、電子透かしデータ入り画像をDCT等を用いて周波数成分に変換する。次に、 $f(i)$ 及び $F(i)$ により、電子透かしデータ $W(i)$ を $W(i) = (F(i) - f(i)) / f(i)$ により計算して抽出する。次に $w(i)$ と $W(i)$ の統計的類似度をベクトルの内積を利用して、 $C = W * w / (WD * wD)$ により計算する。ここで、

$W = (W(1), W(2), \dots, W(n))$ 、
 $w = (w(1), w(2), \dots, w(n))$ 、

(但し、 WD =ベクトル W の絶対値、 wD =ベクトル w の絶対値)である。

【0015】統計的類似度 C がある特定の値以上である場合には該当電子透かしデータが埋め込まれていると判定する。

【0016】この電子透かしを、身分証明書の記載事項から生成し、印刷する写真に埋め込む。検査の時に写真からこの電子透かしを取り出して、記載事項と比較することで、身分証明書が真正か偽造か判別することが可能

である。

【0017】

【発明が解決しようとする課題】上記第1の従来技術では、磁気カードの磁気情報を読み込んで、その磁気情報を当該磁気カード上の磁気記録部分と同じように他の磁気カード上の磁気記録部分に書き込むだけで、同一の磁気カード（同一とみなされる磁気カード）を作ることができるので、容易に第三者が磁気情報をそのまま複製すれば、同一のカードを作成することができる。また、図20に示すような従来の磁気カードID情報暗号化方式においては、磁気カードのID情報を磁気情報として記録しているだけであるので、第三者が容易に当該磁気カードの複製を行うことができる。

【0018】また、カードに写真等が貼る第2の従来技術でも、そのままコピーすれば、同一のカードが作れる。また顔写真と相関の有るデータが印刷されているので、カードの写真データを元に内容を解析され易い。また、この従来技術2では、カードの写真部や暗号化した写真情報部に大きな傷が入ると、真正のカードを偽造カードと誤認してしまう可能性がある。すなわち、写真情報を暗号化したデータを磁気カードに印刷するという従来の方式では、そのままその印刷データをコピーすれば同一の磁気カードを作ることができ、顔写真と相関のあるデータが「写真情報を暗号化したデータ」として印刷されているために、磁気カード上の顔写真を基にそのID情報（写真情報を暗号化したデータ）の内容を解析され易いという問題点がある。

【0019】さらに、第3の従来技術では、偽造防止用の情報が偽造しようとする者に見えるため、そこの重ね合わされている複雑なパターンを模倣して、通常の人がある限りでは偽造かどうか判別できないレベルにもっていくことができる。今日の写真技術、画像処理技術、印刷技術のレベルを考えるとこの偽造防止用のパターンを模倣することは可能である。その結果、身分証明書の記載事項に明白な間違い、例えば、正規の社員番号と桁数が相違、本来はアラビア数字でなければならない社員番号が漢数字になっているなどが無い限り、偽造身分証明書を見分けることは難しい。

【0020】また、第4の従来技術では、身分証明書の記載事項から生成した識別データを写真のうえに重ね合わせる形で印刷している。この方法であれば真正か偽造かを判断することができる。しかし、この場合は記載事項と識別するデータが可視データとなっているため、充分な数のデータを集積すれば、記載事項から識別するデータを生成する計算式を両データから逆算にて導くことが可能となってくる。この計算式が見出されてしまうと当該身分証明書と同じ計算式を用いた身分証明書は、無制限に偽造されることになる。また、写真の中にこの識別データを埋め込んでしまう方法も記載されているが、この実施例では識別データが埋め込まれている位置を固

定しているため、偽造する者からすれば位置を特定しやすい。

【0021】また、第5の従来技術による電子すかしを利用する場合は、元の写真が必要であり、身分証明書とともにこの元の写真をもっていることは通常ありえない。従って、この技術だけで身分証明書の持ち主が正規の持ち主か否かを判断することは困難である。

【0022】本発明の目的は、磁気カードに入れる情報を、磁気データとカードの模様の両方に持たせて、容易に第三者がカードの複製を出来ない様にし、もし複製した場合は容易に判別出来る様にして、セキュリティを向上させることを目的とする。

【0023】また、本発明の目的は、磁気カードに記録／印刷するID情報を、磁気情報の形態と磁気カードの模様とに埋め込む形態との両方の形態で持たせて、第三者が容易に磁気カードの複製をできないようにして、磁気カードに関するセキュリティを向上させることができる磁気カードID情報暗号化方式を提供することにある。

【0024】さらに、本発明の目的は、上記電子すかし技術を利用して、身分証明書の偽造を極めて困難として、たとえ偽造したとしても、簡単に正規の持ち主か否かを判別できることを目的とする。

【0025】

【課題を解決するための手段】本発明の磁気カードの暗号解読方式は、第三者がカードの磁気を不正に複製した場合に、容易に複製したカードであるか判断出来る様に、磁気データの他にカードの模様と情報を入れる手段を設けることにより、不正な複製かどうかを容易に判断する手段を提供する。

【0026】より具体的には、予めオリジナルのカードの模様には、カードの模様の元になる所有者の指紋パターンをFFT（高速フーリエ変換）処理を施して周波数ドメインの情報に変換し、ID情報を、この周波数ドメインの情報でエネルギーの強い周波数成分に加算し、その加算した結果を逆FFT処理で周波数ドメインから2次元の画像イメージに変換して、カードにID情報が埋め込まれている指紋パターンの模様を印刷しておく。

【0027】このカードの指紋パターンを読み取り機で読み込み、その画像をFFT処理で周波数ドメインの情報に変換し、所有者の指紋を読み取り機で読み取り、そのデータにFFT処理を施して周波数ドメインの情報に変換したものととの差分を取り、ID情報を抽出する。

【0028】また、今まで通りカード磁気読み取り機で読み込まれたデータを、復号化して解読しID情報を抽出する。このID情報とカード模様から抽出したID情報とを比較し、同じIDで有ればオリジナルのカードで有り、違うIDで有れば不正に複製したカードであると判断する。

【0029】本発明の磁気カードには、通常の磁気情報の他に、カードの模様にもID情報を入れている。この

ため、磁気データだけを複製しても模様部分を複製しない限り、同一カードとして見なされない。カードの模様から抽出したID情報と磁気データから抽出したID情報を比較することによって、容易にカードの不正な複製を見分けることが可能となる。また、模様にID情報が入っていることは、模様の周波数成分のエネルギーの強いところにID情報が刷り込まれる為、素人が見分けることは不可能となる。もし仮に、模様の違いが分かったとしても、本人の指紋パターンが無い限り、ID情報を抽出することは不可能である。

【0030】さらに、本発明の磁気カードID情報暗号化方式は、磁気カードのID情報を暗号化する暗号化手段と、暗号化されたID情報を磁気情報として当該磁気カードに記録する磁気情報作成手段とを含む磁気カードID情報暗号化方式において、磁気カードの模様の原面パターンを周波数（空間周波数）ドメインの情報に変換する周波数ドメイン変換手段と、当該磁気カードのID情報を周波数ドメインに分布させた情報を生成し、当該生成された情報と前記周波数ドメイン変換手段による変換によって生成された情報とを加算する加算手段と、前記加算手段による加算によって生成された周波数ドメインの情報を2次元の画像パターンに戻す周波数ドメイン逆変換手段と、前記周波数ドメイン逆変換手段によって生成された画像パターンを当該磁気カードの模様として使うように当該磁気カードに印刷する画像パターン印刷手段とを有することを特徴とする。ここで、周波数ドメイン変換手段はFFT（Fast Fourier Transform：高速フーリエ変換）手段またはDCT（Discrete Cosine Transform：離散コサイン変換）手段等によって実現され、周波数ドメイン逆変換手段は逆FFT手段や逆DCT手段等によって実現される。

【0031】さらにまた、本発明によるカード型記録媒体は、カードに印刷する写真をデジタルデータとして取り込み、取り込んだデータをDCT変換をかけて空間周波数に変換し、変換後のデータに当該カードに記載されている事項から生成した識別データに挿入する。当該カードを身分証明書として使用した場合、該身分証明書に挿入されたデータをIDCT変換をかけて通常の写真にもどし、身分証明書に記載されるデータとともに身分証明書に印刷する。検査する際には、身分証明書の写真、記載事項を読み込んで、読み込んだ写真のデータにDCTをかけて空間周波数に変換し、一方、読み込んだ記載事項からは識別データを生成し、両者の相関関係から身分証明書が真正か偽造かを判断する。

【0032】上記の構成をとっているため、身分証明書の写真と識別データ間の相関関係が強い場合は、当該身分証明書は真正であると判断する。また、相関関係が弱い場合は、当該身分証明書は偽造であると判断する。

【0033】更に加えて、本発明は、カード型記録媒体作成システムを電子計算機で動作させるためのプログラ

ムを格納した記録媒体であり、所有者を特定する特定データに基づいて識別データを生成するステップと、貼付されるべき写真画像を、空間周波数データに変換するステップと、前記空間周波数データの各成分と前記識別データの対応する成分とを乗算し、この乗算値を定数倍した値を前記写真画像の空間周波数データの対応する成分に加算し、この加算された空間周波数データを逆変換して画像データに変換するステップと、前記画像データと前記特定データとをカード型記録媒体に書き込むステップとを含むプログラムを格納したことを特徴とする。当該記録媒体には、各ステップ毎に記録媒体に書き込む画像領域とID情報や特定データを書き込むデータ領域にそれぞれ書き込むデータを作成するので、当該記録媒体の作成の容易性や、誤りのない統一的なカードが作成できる。

【0034】

【発明の実施の形態】まず、本発明を実施するための最良の形態について図面を参照して詳細に説明する。

【0035】[第1の実施形態] 本発明による第1の実施形態について説明する。図1を参照すると、カード25に書き込んでいるカード上の書込指紋パターンをカード画像読み取り機6で読み込み、その画像をFFT7で高速フーリエ変換する。一方現在の所持者である自分の指紋パターンを指紋パターン読み取り機10で読み込み、そのデータをFFT11で高速フーリエ変換する。減算器8は、FFT7出力からFFT11出力を減算し、ユーザを特定するID情報9を抽出する。

【0036】また、カード25の磁気データをカード磁気読み取り機1で読み取り、そのデータを復号化処理2によって符号を解読し、ID情報3を抽出する。

【0037】これらのカード25の模様から抽出したID情報9と磁気データから抽出したID情報3とを、比較器4で比較し、その比較結果により、不正に複製したものかどうかを判定回路5が判断する。

【0038】次に、このカード25の作成方法について説明する。このカード25では、図3に示すように、指紋パターン19と磁気ストライプ18が作成されている。このカード25には、カード25の指紋パターンに予めID情報を埋めこんで置く。図2を用いて詳細にID情報の埋めこみ方法について説明する。

【0039】図2において、カード25に印刷する自分の指紋パターン12を、不図示の画像読取装置によって指紋画像信号として読み出し、FFT11で高速フーリエ変換して周波数ドメインに変換して、ID情報9を周波数成分が強い帯域に加算器13で加算する。この場合、強いエネルギーのところに微小なID情報を加算するので、原画像に対しては殆ど影響を与えない。

【0040】次に、その結果を逆FFT14で2次元の画像イメージに変換して、カード25に印刷する模様を作り、指紋パターン印刷機15でカード25に、図3に

示す符号19のように指紋パターンを印刷する。ここで、印刷された指紋パターン19は、見た目では自分の指紋パターン12と区別が出来ない位の画像になり、この模様はID情報が異なっても同じ様に見える。

【0041】また、ID情報9を、暗号化器16で暗号化し、磁気テープ作成機17でカードの磁気ストライプ(図3の18)に磁気情報を作成する。この際、指紋パターン19を書き込むステップと、磁気ストライプへの磁気情報を書き込むステップはいずれを先に行ってもよいが、一体的にマッチさせておく。

【0042】以上の方法で、カードのID情報が、磁気データとカードの指紋パターンの模様の両方に刷り込まれたカードが出来る。

【0043】図1に戻って、上述した方法で作成されたカード25を、先ず、カードの模様を指紋パターン読み取り機6で読み込み、読み込んだ画像をFFT7で高速フーリエ変換して周波数ドメインの情報に変換する。ここで高速フーリエ変換は離散的数値系列のフーリエ変換であり、一般のフーリエ変換に対して計算回数を大幅に短縮できる変換方法である。この高速フーリエ変換をすると、指紋パターン+ID情報の周波数スペクトラムが生成されるが、このスペクトラムは、図4の指紋データスペクトラム+ID情報20のように示される。次に、図1の指紋読み取り機10で読みとられた所有者の指紋パターン12をFFT11で同様に周波数ドメインに変換すると、図4の符号22に示されるような指紋データ周波数スペクトラム22が得られる。減算器8で、指紋パターン+ID情報の周波数スペクトラム20から、指紋データ周波数スペクトラム22を減算すると、ID情報の周波数スペクトラム21に示される様に、ID情報の部分だけ抽出される。

【0044】また、カード25のカード磁気読み取り機1で、磁気データを読み出し、この情報を復号化処理2で符号を解読し、ID情報3を抽出する。カード磁気読み取り機1は、カード25内の指紋パターンを光ヘッドの光電変換手段によって、カード25内の磁気ストライプの磁気情報を磁気ヘッドの磁気/電気変換手段によって、カードと各ヘッドとを相対的に移動して、同時に又は個別に電気信号として読み出すことができる。

【0045】次に、カード25の指紋パターン19の模様から抽出したID情報9とカードの磁気データから抽出したID情報3を比較器4で比較し、判定回路5において、同一のID情報であればそのカードは正規のカードと判定し、異なるID情報であればそのカードは不正に複製したカードと判定する。

【0046】なお、以上の処理は、プログラムを格納したコンピュータ等によって実現できる。すなわち、以上の処理を実行するプログラムを、フロッピーディスク等の記憶媒体に格納させ、この記憶媒体からプログラムをロードしたコンピュータに実行させることもできる。

【0047】また、上記実施形態では、指紋パターンとID情報とをカード型記録媒体に書き込んだ例を示したが、顔写真や目の網膜網等の特徴のある画像とID情報とをペアーとして扱うことで、カード型記録媒体の所持者を正当な所持者と判断でき、カード型記録媒体の偽造を防止し、偽物対策にも有効である。

【0048】また、上記実施形態では、ID情報を磁気ストライプに記録する例を示したが、磁気カードばかりでなく、ICカードであっても良く、例えばID情報をEEPROMやフラッシュメモリ等に格納して上述の作用を適用してもよく、更に他のカード型記録媒体でも同様である。この点は、下記の実施形態でも適時適用できることは勿論である。

【0049】[第2の実施形態]次に、本発明の第2の実施形態について図面を参照して詳細に説明する。なお、本実施形態は、第1の実施形態に従って、更に詳細に且つ具体的に説明するものである。図1を参照すると、カード25の指紋パターン19をカード画像読み取り機6で読み込む。FFT7とFFT11は、25ポイントの周波数帯域に分ける高速フーリエ変換で、各周波数帯域当たりの量子化数は16ビットとする。このFFT7でカードから読み取った指紋パターン19を高速フーリエ変換したものから、指紋読み取り機10で読み取った自分の指紋パターンをFFT11で高速フーリエ変換したものを、減算器8で減算し、32ビットのユーザを特定するID情報9を抽出する。

【0050】また、カード25の磁気データ18をカード磁気読み取り機1で読み取り、そのデータを復号化2によって符号を解読し、32ビットのID情報3を抽出する。

【0051】これらのカード25の指紋パターン19の模様から抽出した32ビットのID情報9と、磁気データ18から抽出した32ビットのID情報3を、比較器4で比較し、同一の時は"0"を出力し、異なる時は"1"を出力して、判定回路5において、"0"の時は正規のカードで、"1"の時は不正に複製したカードであると判定する手段により構成される。

【0052】先ず、カード25の指紋パターン19の模様に予め32ビットのID情報を埋めこんで置く。図2を用いて詳細にID情報の埋めこみ方法について説明する。カードに印刷する自分の指紋パターン12を、FFT11で周波数ドメインに変換して、32ビットのID情報9を周波数成分が強い帯域に加算器12で加算する。FFT11は、25ポイントの周波数帯域に分ける高速フーリエ変換で、各周波数帯域当たりの量子化数は16ビットとする。この場合、強いエネルギーのところに微小なID情報を加算するので、自分の指紋パターンに対しては殆ど影響を与えない。この時の加算の方法は、32ビットのID情報を4ビット×3ケ、3ビット×4ケ、2ビット×4ケに分けて、原画像の周波数成分

のエネルギーの強いところから順番に加算していく。次に、その結果を逆FFT14で2次元の画像イメージに変換して、カードに印刷する模様を作り、指紋パターン印刷機15でカードに指紋パターンを印刷する。ここで、印刷された画像イメージは、見た目では自分の指紋パターン12と区別が出来ない位の画像になり、この模様はID情報が異なっても全て同じ様に見える。

【0053】また、32ビットのID情報9を、暗号化器16で暗号化し、磁気テープ作成機17でカード25に磁気情報を作成する。

【0054】以上の方法で、32ビットのID情報9が、磁気データ18とカードの指紋パターン19の模様の両方に刷り込まれたカードが出来る。

【0055】上述した方法で作成したカード25を、まず、カード25の指紋パターン19の模様を指紋パターン読み取り機6で読み込み、その画像をFFT7で周波数ドメインの情報に変換すると、指紋パターン+ID情報周波数スペクトラム20のように示される。次に、図4に示すように、自分の指紋パターン12をFFT11で周波数ドメインに変換すると、指紋データ周波数スペクトラム22に示されるようになり、減算器8で、指紋パターン+ID情報の周波数スペクトラム20から、指紋データ周波数スペクトラム22を減算すると、図5に示す様に周波数成分の強いところに、ID情報21に示される様に、ID情報21の部分だけ抽出される。このID情報21だけのスペクトラムを、例えば4ビット×3ケ、3ビット×4ケ、2ビット×4ケに分けて、予めカードに書き込んだ時の順番と逆の手順でデータを並べ替えて、32ビットのID情報に戻す。

【0056】また、図1に示すように、カードの磁気読み取り機1で、磁気データを読み出し、この情報を復号化処理2で符号を解読し、32ビットのID情報3を抽出する。

【0057】次に、カード25の指紋パターンの模様から抽出した32ビットのID情報9とカードの磁気データから抽出した32ビットのID情報3とを比較器4で比較し、同一のID情報であれば"0"を出力し、異なる場合は"1"を出力する。この値を判定回路5において、"0"の時は正規のカードであるため、通常のカード処理に引き続き移行し、"1"の時は不正に複製されたカードであるためカードの処理を中止する作業を行う。

【0058】〔第3の実施形態〕次に、本発明の第2の実施の形態について図面を参照して説明する。図6を参照すると、図1と基本的には原理は同じで、図1のFFTに相当する部分にJPEG等の画像圧縮で使用しているDCT（離散コサイン変換）を用いる。このDCTは、直交変換符号化の一種で、DFT（Discrete Fourier Transform）の改造版で、8画素×8画素のブロック毎に直交変換行列で変換し変換結果を量子化して符号化

データに置き換えて符号化する。このDCTはFFTと同様にバタフライ演算で演算処理を高速化でき、画像成分の高域成分の少ない特性を利用している。本実施形態で用いるDCTには、非線形量子化して等長符号化する方式や準線形量子化して可変長符号化する方式のいずれでもよい。なお、画像圧縮するブロックによって符号化誤差が違うとそのブロックが画面上でブロック歪として現れるので、このブロック歪が目立ちやすい画面の場合には符号化速度を高くし、目立たない画面の場合には符号化速度を低くして全体を通しての画質を一定にできるという特質を有している。

【0059】このDCT23、24のデータ変換時、第1の実施形態では、指紋パターンの全ての情報に対して周波数ドメインの変換をしていたが、第2の実施形態では、カードの模様を作る時に、予め自分の指紋パターンを8×8ドットの細かい画像（ブロック）に分けてから、DCTを用いて刷り込んでおく。この場合、ID情報9は、指紋パターンを8×8ドットに細かく分けた領域全てにID情報が刷り込まれている為、カードに傷がついたり、自分の指紋に多少の傷が有っても、傷の付いていない部分のデータの相関関係により、たとえば多数決処理には、ある程度の傷で有ればID情報を抽出することが出来るという新たな特徴が生まれる。

【0060】また、指紋パターンのFFT又はDCTによる画像信号の周波数スペクトラムの特定周波数成分にID情報を加算する例を示したが、指紋パターンの特徴的な領域と範囲を特定することで、現実の指紋採取時の指紋パターンの取得領域や範囲を合わせる必要があるが、この点は、指紋読み取り器10の採取特性に従うことで解決できる。

【0061】〔第4の実施形態〕本発明の第4の実施形態は、磁気カードID情報暗号化方式に関するもので、カード型記録媒体として、磁気カードを用いる。

【0062】図7は、磁気カードID情報暗号化方式の構成を示すブロック図である。本実施形態の磁気カードID情報暗号化方式は、磁気カードに印刷される模様の元になる原画パターン31をFFT（高速フーリエ変換）して、周波数ドメインの情報（原画像周波数スペクトラム39。図8参照）に変換するFFT手段32と、当該磁気カードのユーザを特定するID情報36を周波数ドメインに分布させた情報（ID情報周波数スペクトラム41。図8参照）を生成して原画像周波数スペクトラム39とID情報周波数スペクトラム41とを加算する加算手段33と、加算手段33による加算によって生成された周波数ドメインの情報である原画像+ID情報周波数スペクトラム40（図8参照）を2次元の画像パターンに戻す逆FFT手段34と、逆FFT手段34によって生成された画像パターンを当該磁気カードの模様（図10参照）として使うように当該磁気カードに印刷する画像パターン印刷手段35と、ID情報36の内容

を暗号化する暗号化手段37（暗号化の態様は問わない）と、暗号化されたID情報36を磁気情報として当該磁気カード上の磁気ストライプ（図10参照）等の磁気記録部分に書き込む磁気情報作成手段38とを含んで構成されている。

【0063】ここで、暗号化手段37による暗号化の態様として、対称暗号系（慣用暗号系）によるDES、MULTI2等のブロック暗号やバーナム暗号、入替え暗号等の同期式等のストリーム暗号でもよく、非対称暗号系（公開鍵暗号）によるRAS、Rabin等のベキ乗剰余型暗号やナップザック型暗号等であってもよく、特に使用の制限がなければ、限定されるものではない。

【0064】以下に、図7中の構成要素について説明を加える。FFT手段32は、例えば25ポイントの周波数帯域に分けるFFTを行う。ここで、各周波数帯域当たりの量子化数は、例えば16ビットとする。暗号化手段37は、例えば32ビットのID情報36を暗号化する（後述の図9参照）。

【0065】なお、暗号化手段37と磁気情報作成手段38とは、上述の第1の従来技術で説明した同名の手段（図20参照）と同一の手段であってもよい。

【0066】図8は、本実施例の磁気カードID情報暗号化方式の原理を説明するための図である。また、図9は、加算手段33の処理（ID情報36の分割処理等）を説明するための図である。

【0067】さらに、図10は、本実施形態の磁気カードID情報暗号化方式によって製造される磁気カード42の一例を示す図である。磁気カード42には、ID情報を刷り込んだ模様44と、ID情報を暗号化したデータを記録した磁気ストライプ43から構成されている。この磁気カード42の所有者は、自分自身を証明する身分証明書や銀行用のキャッシュカード、クレジットカード等に個別に、又は統括的に所持して提示することによって種々使用できる。

【0068】また、図11は、本実施形態の磁気カードID情報暗号化方式の処理を示す流れ図である。この処理は、FFTステップ501と、ID情報周波数スペクトラム生成ステップ502と、原画像+ID情報周波数スペクトラム生成ステップ503と、逆FFTステップ504と、画像パターン印刷ステップ505と、暗号化ステップ506と、磁気情報記録ステップ507とからなる。

【0069】次に、このように構成された本実施例の磁気カードID情報暗号化方式の動作について、図7～図11を参照して詳細に説明する。

【0070】まず、磁気カードに印刷される模様の元となる原画像パターン31が用意される。このときに、この原画像パターン31は、後で周波数ドメインの情報に変換した時に、ID情報36を加算してもオーバーフローしないものを予め準備しておく。

【0071】FFT手段32は、この原画像パターン31に対して、周波数ドメインの情報になるように、高速フーリエ変換（FFT）を行う（図11のステップ501）。これによって、図8に示すように、原画像パターン31は原画像周波数スペクトラム39に変換される。

【0072】加算手段33は、FFT手段32によって生成された原画像周波数スペクトラム39の分布状況を見て、図8や図9に示すように、ID情報周波数スペクトラム41を生成する（ステップ502）。すなわち、本実施形態のようにID情報36が32ビットである場合には、この32ビットを4ビット×3、3ビット×4、および2ビット×4というように分けて、原画像周波数スペクトラム39の分布状況に類似させて、ID情報周波数スペクトラム41を生成する。即ち、原画像パターン31の周波数成分のエネルギーがより強い部分から順番に、分割したID情報36のビット数のより多い部分を分布させて、ID情報周波数スペクトラム41を生成する。ただし、このような「原画像周波数スペクトラム39の分布状況とID情報周波数スペクトラム41の分布状況とを類似させる処理」を行わなくても、本実施形態を実現することは可能である。

【0073】次に、加算手段33は、図8に示すように、原画像周波数スペクトラム39とID情報周波数スペクトラム41とを加算して、原画像+ID情報周波数スペクトラム40を生成する（ステップ503）。

【0074】この場合に、原画像周波数スペクトラム39のエネルギーに比べてID情報周波数スペクトラム41のエネルギーは微小なものとなるように設定されているので、磁気カード上の模様となる画像パターンに対してID情報36（ID情報周波数スペクトラム41）の存在はほとんど影響を与えない。また、本実施形態では、原画像周波数スペクトラム39とID情報周波数スペクトラム41との両方の分布状況ができるだけ類似した形状とされるので（図8参照）、磁気カードの模様の画像パターンに及ぼされるID情報36の影響は、さらに小さくなる。

【0075】逆FFT手段34は、ステップ503で生成された原画像+ID情報周波数スペクトラム40に対して逆FFTを行い、原画像+ID情報周波数スペクトラム40を画像パターンに戻す（ステップ504）。ここでできた画像パターンは、上述のように、見た目では原画像パターン31と非常に区別が付きにくい画像パターンになる。

【0076】画像パターン印刷手段35は、この画像パターンを模様として磁気カードに印刷する（ステップ505）。このように作成（印刷）された磁気カードの模様は、原画像パターン31が同一であればID情報36が異なっても全て同じように見える。

【0077】一方、暗号化手段37は、磁気カードに記録する磁気情報を従来技術によって作成する要領で（図

20参照)、ID情報36のデータを分析しにくくする暗号化を行う(ステップ506)。

【0078】磁気情報作成手段38は、ステップ506で暗号化されたID情報を示す磁気情報を磁気カード上の磁気記録部分(図10中の磁気ストライプ)に書き込む(ステップ507)。以上で、磁気カードのID情報36が、磁気情報と模様との両方の態様で記録/印刷される(刷り込まれる)。

【0079】上記実施形態では、記録媒体の磁気カードに原画パターンにID情報を加算して、表面的に見える磁気カードの画像信号には原画パターンと殆ど見分けのつかないようにしているが、この暗号化された磁気カードは、特定の読取器によってID情報を読み取り、現実の磁気カードの所持者が示すID情報と一致するのかどうかで正規か、又は不正に磁気カード保持者かが判断できる。

【0080】[第5の実施形態]本発明の第5の実施形態による磁気カードID情報暗号化方式について、説明する。

【0081】図12は、本発明の磁気カードID情報暗号化方式の第5の実施形態の構成を示すブロック図である。本実施形態の磁気カードID情報暗号化方式は、磁気カードに印刷される模様の元になる原画パターン61をDCTで周波数ドメインの情報に変換するDCT手段62と、当該磁気カードのユーザを特定するID情報66を周波数ドメインに分布させた情報を生成して、当該生成情報とDCT手段62によって生成された周波数ドメインの情報とを加算する加算手段63と、加算手段63による加算によって生成された周波数ドメインの情報を逆DCTによって2次元の画像パターンに戻す逆DCT手段64と、逆DCT手段64によって生成された画像パターンを当該磁気カードの模様として使うように当該磁気カードに印刷する画像パターン印刷手段65と、ID情報66の内容を暗号化する暗号化手段67(暗号化の態様は問わない)と、暗号化されたID情報66を磁気情報として当該磁気カード上の磁気ストライプ等の磁気記録部分に書き込む磁気情報作成手段68とを含んで構成されている。

【0082】なお、本実施形態における加算手段63、画像パターン印刷手段65、暗号化手段67、および磁気情報作成手段68は、第4の実施形態における加算手段33、画像パターン印刷手段35、暗号化手段37、および磁気情報作成手段38と同様の手段である。

【0083】図12に示すように、本実施形態の磁気カードID情報暗号化方式の原理は、図8に示す第4の実施形態の原理と基本的には同じである。ただし、本実施例では、図7中のFFT手段32に相当する部分にJPE G (Joint Photographic Coding Experts Group)等の画像圧縮で使用されているDCT(後述のように、原画パターン61を細分化原画パターンに細分化した上で

のDCT)を行うDCT手段62が用いられ、逆FFT手段34に相当する部分に逆DCTを行う逆DCT手段64が用いられる。

【0084】次に、本実施形態に特徴的な動作について、詳細に説明する。第4の実施形態におけるFFT手段32は、原画パターン31の全ての情報を対象として周波数ドメインの情報への変換を行っていた。しかし、本第2の実施形態におけるDCT手段62は、原画パターン61を8×8ドットの細かい画像パターンである細分化原画パターンに分けて、各細分化原画パターンに対してDCTを行う。

【0085】また、加算手段63は、ID情報66を周波数ドメインに分布させた上で、その周波数ドメインのID情報66を各細分化原画パターンにDCTが施された情報のそれぞれに加算する。

【0086】本実施形態の磁気カードID情報暗号化方式では、上述のように細分化原画パターンの全てにID情報66が刷り込まれるため、磁気カードに部分的に傷がついて一部の画像のデータがおかしくなっても、傷のついていない画像の部分には依然として正確なID情報66が刷り込まれたままとするという特長が生まれる。

【0087】上記磁気カードID情報暗号化方式の読取方式の一例を、図13に示して説明する。正確なID情報66が刷り込まれた模様44の画像データとID情報を暗号化したコードとして記録されている磁気ストライプ43を含むカード型記録媒体42を磁気カード情報読取器の所定の個所に挿入する。磁気読取部81では、磁気カード42と相対的に移動する磁気ヘッドで磁気ストライプ43に記録されている記録コードを電気信号に変換する。記録コードは逆暗号化手段82で上記暗号化手段67で暗号化した方式と逆の方式で暗号化を正規のID情報信号に変換し、ID情報83を得る。一方、画像読取部84では、予め定められた模様44の領域を光電変換素子で直接又は、縮尺して画像信号として読み取る。当該画像信号は小ブロック毎に、上記DCT手段62と同様に、DCT手段85でDCTを行い、次に、DCTされた画像信号は、ID情報83の周波数スペクトラム化したデータから差を取られ、逆DCT手段87で先のDCT手段85と逆の変換を行い、抽出パターン88を得ることができる。

【0088】次に、例えばこのカード型記録媒体を所持する人の顔を写真撮影等で取得したり、著作物の原画そのものを原画パターン89としてデジタル変換し、抽出パターンのデジタル信号と比較器90で比較する。この比較の結果、両者に差異がなく同一模様であると判断された場合には、正規のカード保持者であると認証される。また、両者の差異が大きかった場合には、正規のカード保持者ではないと判断される。

【0089】この際、検出されたID情報83と、本磁気カードの所有者が示すID情報とが一致しておれば、

当該原画パターンの所有者が一致していると判断できる。他方、一致しなければ、本磁気カードの所有者は拾得された磁気カードか、不正行為の所有者と判断できる。このように、例えば原画パターンそのものが貴重な著作権を有する著作物であれば、その原画パターンが上述したように本磁気カードに刷り込まれている場合には、真の所持者であるのかどうかを即座に判断でき、磁気カードの偽造及び不正使用を摘出し、セキュリティの向上に寄与できる。

【0090】上記暗号解読器は、図12に示す磁気カードID情報暗号化方式に対応する例を示したが、図7に示す第4の実施形態の磁気カードID情報暗号化方式であっても、DCT手段85と逆DCT手段87とを、FFT手段32と逆FFT手段34に変更することで、解読することができる。

【0091】〔第6の実施形態〕図14は、本発明の第6の実施形態のカード型記録媒体の一種の身分証明書を作成する構成と信号経路を示し、図15は、本発明の第6の実施形態の身分証明書を検査する検査工程とその構成図である。図16は、本発明の第6の実施形態の身分証明書を発行するためのシステムを示し、図17は、本発明の第6の実施形態の身分証明書を検査するシステムを示す。

【0092】図14において、写真100は、身分証明書の正規の所有者の写真である。記載事項110は当該身分証明書220に記載される事項で、公務員や会社社員用身分証明書の場合には、所有者の名前、部署の名前、登録番号や社員番号などが記載される。学生用身分証明書の場合には、所有者の名前、学部の名前、学生番号などが記載される。キャプチャ120は、写真100を画像データとして取り込む画像読み取る部分である。識別データ生成部130は、身分証明書220の記載事項110から計算によって識別データを生成する。生成の方法としては、名前や社員番号に基づいて乱数を発生させる方法が使用できる。DCT部140は、キャプチャ120で取り込まれた画像データを空間周波数成分に変換する機能を有する。部分平均計算部150は空間周波数成分の近傍3点の絶対値の平均を計算する。この部分平均は乗算器160で識別データと乗算され、この乗算結果は乗算器180で定数 α で α 倍される。乗算器180出力は、加算器190で、DCT部140の出力と加算され、この加算結果はIDCT (Inverse Discrete Cosine Transform) 部200に供給される。定数 α はスケールングファクタである。IDCT部200は空間周波数から人間の目に見える画像データに変換する機能を有する。写真210は識別データが埋め込まれている写真であり、この写真210と記載事項110を印刷したものが身分証明書220である。

【0093】次に、作成された身分証明書を現実の使用状態に置かれたときの証明・検査手段について説明す

る。図15において、身分証明書300は、識別データが埋め込まれている写真と、識別データを生成するもとなった記載事項とともに印刷された身分証明書である。キャプチャ310は、この身分証明書の写真の画像部分を光電変換して読み込んで、写真の部分は画像データとして、記載事項の部分も画像データとして分離する機能を有する。DCT部320は、キャプチャ310で分離された画像データを空間周波数成分に変換する機能を有する。文字認識部330は、キャプチャ310から分離された記載事項部分の画像データから文字認識を用いて、記載事項を文字に変換する。部分平均計算部340はこの空間周波数成分で近傍3点の絶対値の平均値を計算する。

【0094】また、識別データ生成部370は、キャプチャ310から分離された記載事項のデータを元に識別データを計算する。内積計算部380は画像の空間周波数成分から抜き出した識別データと記載事項から生成した識別データとの内積を計算する機能を有する。なお、除算器350、加算器360の動作は後述する。

【0095】以下、身分証明書の作成動作、検査動作をより具体的に詳細に説明する。まず、身分証明書作成の方から説明する。身分証明書を作成する必要のある者が写真100と、識別データを作成する為に必要な記載事項を用意する。ここでは記載事項を社員番号とする。身分証明書作成担当者は、図16(a)のカメラ800、または、スキャナ810で写真100を画像処理装置830に取り込む。

【0096】また、記載事項110はキーボード820から身分証明書作成担当者が入力する。画像処理装置830に取り込まれた写真110の画像データ、及び、記載事項データ110は、図14の流れにそって処理される。取り込まれた画像データはDCT部140で空間周波数成分に変換される。識別データ生成部130ではキーボード820から入力された記載事項データに基づいて平均0、分散1の正規分布の識別データを生成する。空間周波数成分に変換されたデータと識別データとの間で次の計算を行って、識別データを埋め込む。

【0097】DCT部140のDCT後の空間周波数成分の低いものから順に、

$$f(1), f(2), \dots, f(n),$$

識別データを

$$w(1), w(2), \dots, w(n)$$

とし、

$$F(i) = f(i) + \alpha \times \text{avg}(f(i)) \times w(i)$$

を各*i*について計算する。部分平均 $\text{avg}(f(i))$ は前述の部分平均計算部150で計算される。

【0098】IDCT部200は計算結果の $F(i)$ を逆コサイン変換して、識別データが埋め込まれた状態の写真210を作成する。写真210と記載事項110は

印刷装置840で身分証明書に印刷され、身分証明書220ができあがる。

【0099】なお、図16(a)において、ROM835には、図16で示した画像処理装置830の処理を実行させるためのプログラムが格納されている。このROM835はハードディスクやフロッピーディスク等でも代替できる。

【0100】次に、身分証明書を検査する方を説明する。識別データが埋め込まれた写真と記載事項との両方が印刷された身分証明書を、図16(b)のカメラ850で読み込んで、検査装置870に入力する。検査装置870に取り込まれたデータは、図15の流れにそって処理される。読み込まれた画像データは、キャプチャ310で写真の部分と記載事項の部分に分離され、それぞれDCT部320、文字認識部330に出力される。DCT部320は入力されたデータを空間周波数に変換する。

【0101】DCT部320で空間周波数変換後の周波数成分の低いものから順に

$F(1), F(2), \dots, F(n)$

とする。部分平均計算部340は、 $F(i)$ の近傍3点の絶対値の部分平均 $avg(F(i))$ を計算する。画像データから抜き出す識別データを $W(i)$ とし、

$W(i) = F(i) / avg(F(i))$ により計算する。加算器360はこの $W(i)$ について、画像全体の総和 $WF(i)$ を i 毎に計算する。

【0102】一方、文字認識部330は、記載事項部分の画像データから文字認識にて記載事項を文字として再生する。識別データ生成部370は文字認識部330からの記載事項データに基づいて、平均0、分散1の正規分布の識別データを生成する。

【0103】つぎに、内積計算部380は、識別データ $W(i)$ と $WF(i)$ のベクトル内積を計算する。すなわち、

$C = (WF \times w) / (WFD \times wD)$

を計算する。ここで、

$WF = (WF(1), WF(2), \dots, WF(n))$ 、

$w = (w(1), w(2), \dots, w(n))$ 、

WFD はベクトル WF の絶対値、 wD はベクトル w の絶対値である。この C がある値以上である場合は、写真に埋め込まれた識別データと記載事項との間に相関関係があると判断され、この身分証明書は真正のものであるとディスプレイ880に表示される。

【0104】なお、図16(b)において、ROM875には、図15で示した動作を検査装置870に実行させるためのプログラムを格納している。

【0105】次に、偽造された場合はどうか説明する。一番簡単な偽造方法は写真のみを貼りかえることである。ところが、検査の段階で画像データから抜き取った識別データと記載事項から生成した識別データとで相

関関係を求めたときに、前述の C の値がほとんどゼロになる。なぜなら、写真の中には記載事項に基づいて生成された識別データが埋め込まれていないからである。したがって、容易に偽造身分証明書として判断することが可能である。

【0106】次に考えられる偽造方法は、記載事項から識別データを生成して写真に埋め込み、これを印刷して偽造する場合である。この場合は、識別データを生成する乱数の計算式がわからないので、正規の場合と違う識別データを生成することになり、検査段階での相関関係を示す C の値がゼロになり、偽造身分証明書と判断することが可能である。

【0107】さらに考えられる偽造方法は、写真の1画素1画素を丹念に調べて識別データを取り出し、計算式を割り出す方法である。この場合は、識別データが挿入されるのは空間周波数成分に分解された時であり、これをIDCTした後の写真では調べることは不可能である。つまり、特定の画素の部分に識別データが埋め込まれているわけではないからである。

【0108】上記実施形態では、電子透かし方式に、更に解読の困難な方式を用いたが、更にデータ・ハイディング方式として、損失を伴うデータ圧縮手法(Lossy Compression)や情報損失を伴わないデータ圧縮手法(Lossless Compression)やスペクトラム拡散技術を用いてさらに解読の困難な方式、即ち、それだけ偽造の困難な方式としてもよい。

【0109】[第7の実施形態] 次に本発明の第7の実施形態について説明する。図17は、本発明の第7の実施形態におけるカード型記録媒体の一種の身分証明書を作成する流れを示し、図18は、本発明の第7の実施形態における身分証明書を検査する流れである。図19(a)は、本発明の第7の実施形態の身分証明書を発行するためのシステムを示し、図19(b)は、本発明の第7の実施形態の身分証明書を検査するシステムを示す。

【0110】第7の実施形態では、身分証明書520に磁気記録部分530を設け、この磁気記録部分に名前や社員番号を記録し、身分証明書の表面にはこれらを記載しないようにしたものである。つまり、図17、図19(a)に示すように、識別データを埋め込んだ写真を作成するところまでは、第6の実施形態と同じであるが、身分証明書にする際には、写真100は表面に印刷し、名前や社員番号の記載事項110は、一方は識別データとして写真の画像データに埋め込むが、他方は識別データを直接に、又は暗号化して磁気記録データに変換し、磁気記録部分530に磁気カードライター950を使用して記録する。

【0111】つぎに、検査装置の方は、図18、図19(b)に示すように、身分証明書600内の写真は第6の実施形態と同じで、カメラ850で読み込み、名前な

どの情報は磁気記録部分 610 から磁気カードリーダー 970 を経由して読み込む。読み込んだあとの処理は第 6 の実施形態と同じで、写真をキャプチャ 310 で画像データに変換し、これを各ブロック毎に DCT 変換して、DCT データをこれの部分平均で除算し、この結果を加算して画像全体の総和 WF (i) を求め、磁気カードに記録された識別データのベクトル内積を計算する。この結果で正規の所持者か、又は不正に改造した身分証明書かを判断する。この様に、磁気カードの磁気ストライプ部に識別データ、又は識別データを暗号化したデータを記録するので、こうすることにより、識別データを作成する元となる名前などのデータがわかり難くなり、より偽造することが困難になる。

【0112】上記実施形態では、電子すかし技術を利用して、更に偽造を困難とするもので、上記身分証明書には、顔写真に識別コードを透かしこんだ例を示したが、顔写真に限らず個人を特定できる指紋や目の網膜網を用いてもよく、識別コードの代わりに個人の記憶を尊重する ID 情報としてもよい。

【0113】また、上記各実施形態では、カード型記録媒体に、画像情報と識別 ID 情報とを暗号化技術とを組み合わせて、本人の所持するカードと真のカード所持者の一致を第 1 目的としているが、クレジットカードやテレホンカード、キャッシュカード、社員カード、学生カード、健康保険カードなど今後発行される新規のカードをも含めて、多数のカードに適用できるものである。また、基本的に磁気ストライプに書き込んで読み出す磁気を利用したものがローコストで信頼性も高いが、記録方式には、光学的方式、光磁気方式等、他の方式であっても本発明を利用することができ、上記実施形態に限られるものではないことは明らかである。

【0114】

【発明の効果】本発明によれば、磁気カードの情報と ID 情報を刷り込んだ画像情報の二重で ID 情報を照合出来るということである。これにより、カードを判断する時に、不正にカードを複製したのか、オリジナルのカードであるのか判断し易くなる。その理由は、磁気カードの磁気の部分の他に ID 情報が入っているとは悟られないように、カードの模様 ID 情報を刷り込むようにしたからである。

【0115】また、磁気カードの磁気の部分のデータが壊れても ID 情報の確認が容易に確認することが可能ということである。これにより、外部からの磁気の影響で磁気データが壊れても、模様の部分に ID 情報が刷り込んである為、その情報を読み取って、オリジナルのカードであるか判別することが出来るようになる。その理由は、模様の部分は磁気の影響を受けず ID 情報が壊れないようになっているからである。

【0116】さらに、本発明によると、磁気情報と画像情報との二重の形態で磁気カードに ID 情報を記録/印

刷することができるので、当該磁気カードの複製が困難になり、第三者による磁気カードの偽造を防ぐことができるということである。このような効果が生じる理由は、磁気カードの磁気記録部分の他に ID 情報が入っているとは悟られないように磁気カードの模様 ID 情報を刷り込むようにできるからである。すなわち、本発明の磁気カード ID 情報暗号化方式によって製造された磁気カードは、磁気情報だけを複製しても模様の部分を複製しない限り、同一の磁気カードとしてみなされないもので、磁気カードの偽造は極めて困難なものとなる。なお、模様 ID 情報が入っていることを素人が見分けることは、模様の原画像パターンに係る周波数成分のエネルギーが ID 情報に係る周波数成分のエネルギーよりも強いことに起因して非常に難しいものとなる。また、もし仮に、模様の違いが分かったとしても、原画パターンがない限り、誰も模倣することは不可能である。

【0117】また、磁気カードの磁気記録部分のデータが壊れても ID 情報の確認を容易に行うことが可能になるということである。これにより、外部からの磁気の影響で磁気情報が壊れても、模様の部分に刷り込んである ID 情報を読み取って磁気情報の ID 情報を元に戻すことが簡単にできるようになる。このような効果が生じる理由は、模様の部分は磁気の影響を受けず磁気的原因では模様 ID 情報に刷り込まれた ID 情報が壊れないようになっているからである。

【0118】さらにまた、この発明を用いるとカード型記録媒体の一種の身分証明書を偽造することは困難である。たとえ、身分証明書の顔写真を張り替えたとしても、又は顔写真の画像に識別コードを埋め込んだりして偽造されたとしても、簡単に識別することができる。

【0119】また、本発明による記録媒体には、カード型記録媒体の検査システムをマイクロコンピュータ等にて同一手順で動作させ得るプログラムを格納しているので、指紋や顔等の個人情報の特定ばかりでなく、著作物等の管理にも簡単な設備で適用できる。

【図面の簡単な説明】

【図 1】本発明のカード型記録媒体の判定手段のブロック図である。

【図 2】本発明の実施形態のカード作成フローである。

【図 3】本発明の実施形態のカード図である。

【図 4】本発明の原理図である。

【図 5】本発明の実施形態の ID 情報抽出図である。

【図 6】本発明の一実施形態のブロック図である。

【図 7】本発明の磁気カード ID 情報暗号化方式の第 1 の実施形態の構成を示すブロック図である。

【図 8】図 7 に示す磁気カード ID 情報暗号化方式の原理を説明するための図である。

【図 9】図 7 中の加算手段による処理 (ID 情報の分割処理等) を説明するための図である。

【図 10】図 7 に示す磁気カード ID 情報暗号化方式に

よって製造される磁気カードの一例を示す図である。

【図 11】図 7 に示す磁気カード ID 情報暗号化方式の処理を示す流れ図である。

【図 12】本発明の磁気カード ID 情報暗号化方式の第 5 の実施形態の構成を示すブロック図である。

【図 13】本発明の磁気カード ID 情報暗号化方式の第 5 の実施形態の構成を示すブロック図である。

【図 14】本発明の第 6 の実施形態の身分証明書作成の処理の流れを示す図である。

【図 15】本発明の第 6 の実施形態の身分証明書検査の処理の流れを示す図である。

【図 16】各々、本発明の第 6 の実施形態の身分証明書作成システム、身分証明書検査システムの構成例を示す図である。

【図 17】本発明の第 7 の実施形態の身分証明書作成の処理の流れを示す図である。

【図 18】本発明の第 7 の実施形態の身分証明書検査の処理の流れを示す図である。

【図 19】本発明の第 7 の実施形態の身分証明書作成システム、身分証明書検査システムの構成例を示す図である。

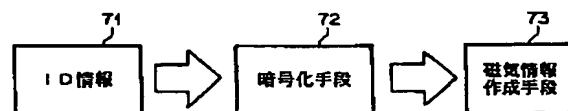
【図 20】従来の磁気カード ID 情報暗号化方式の一例の構成を示すブロック図である。

【符号の説明】

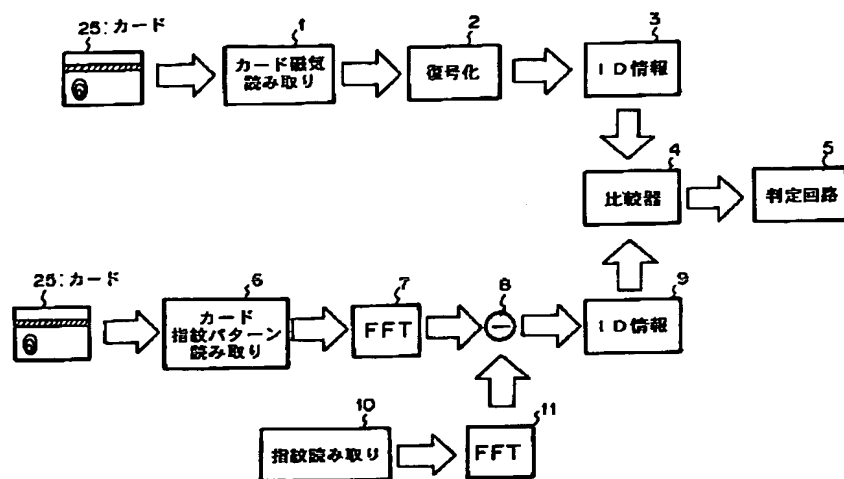
- 1 カード磁気読み取り
- 2 復号化
- 3 ID 情報
- 4 比較器
- 5 判定回路
- 6 カード画像パターン読み取り機
- 7 FFT (高速フーリエ変換)
- 8 減算器
- 9 ID 情報
- 10 指紋読み取り
- 11 FFT
- 12 本人の指紋パターン
- 13 加算器
- 14 逆 FFT
- 15 指紋パターン印刷機
- 16 暗号化
- 17 磁気テープ作成機

- 18 カードの磁気情報
- 19 カードの指紋パターン
- 20 指紋データ + ID 情報の周波数スペクトラム
- 21 ID 情報の周波数スペクトラム
- 22 指紋データの周波数スペクトラム
- 23 DCT (離散コサイン変換)
- 24 DCT
- 31, 61 原画パターン
- 32 FFT 手段
- 33, 63 加算手段
- 34 逆 FFT 手段
- 35, 65 画像パターン印刷手段
- 36, 66 ID 情報
- 37, 67 暗号化手段
- 38, 68 磁気情報作成手段
- 39 原画像周波数スペクトラム
- 40 原画像 + ID 情報周波数スペクトラム
- 41 ID 情報周波数スペクトラム
- 62 DCT 手段
- 64 逆 DCT 手段
- 120, 310 キャプチャ
- 130, 370 識別データ生成部
- 140, 320 離散コサイン変換部 (DCT)
- 150, 340 部分平均計算部
- 160, 180 乗算器
- 190, 360 加算器
- 200 逆離散コサイン変換部 (IDCT)
- 330 文字認識部
- 380 内積計算部
- 390 相関比率計算部
- 630 磁気カードリーダー
- 800, 850 カメラ
- 810 スキャナ
- 820, 860 キーボード
- 830, 930 画像処理装置
- 840 印刷装置
- 835, 875, 935, 995 ROM
- 870, 990 身分証明書検査装置
- 880 ディスプレイ
- 950 磁気カードライター
- 970 磁気カードリーダー

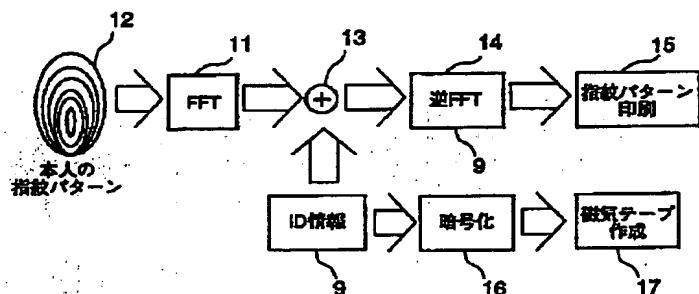
【図 20】



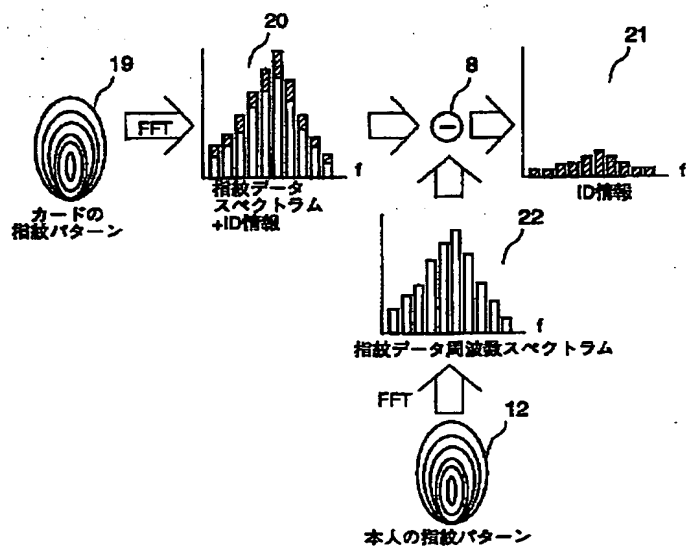
【図1】



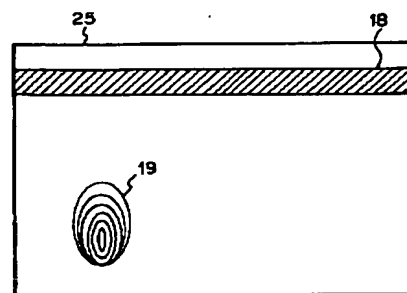
【図2】



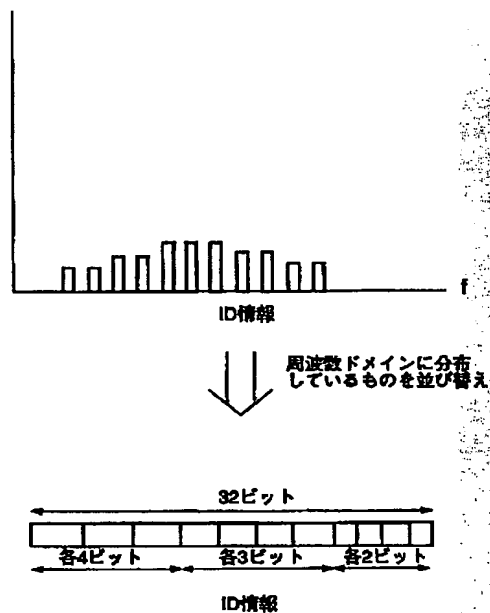
【図4】



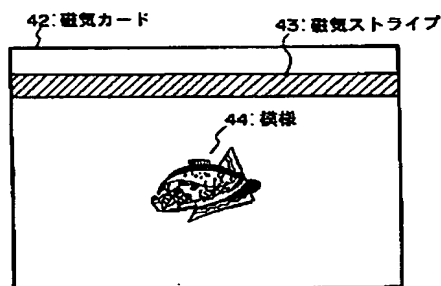
【図3】



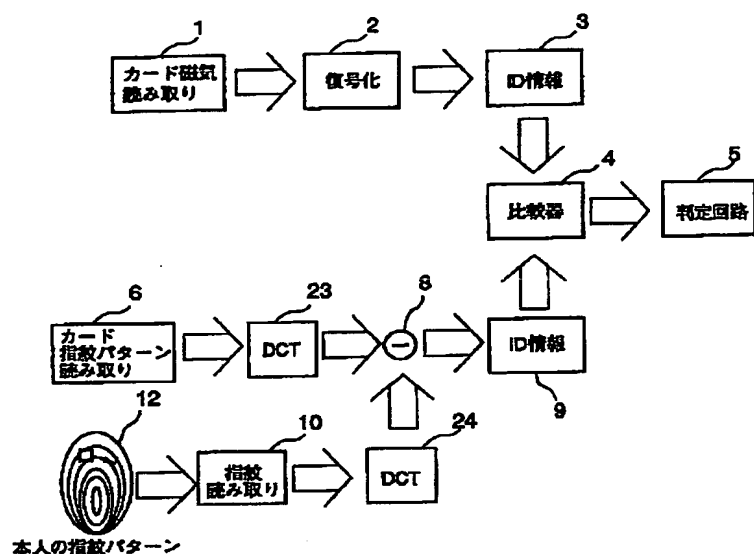
【図5】



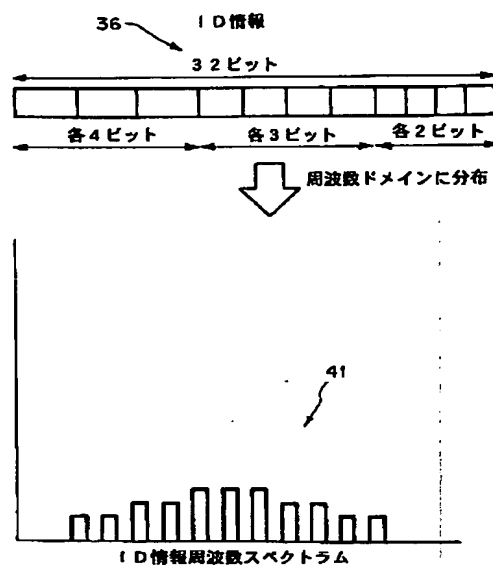
【図10】



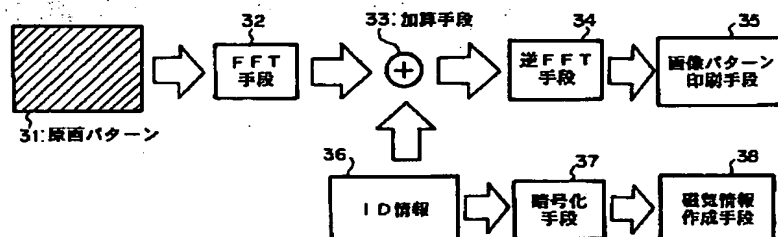
【図 6】



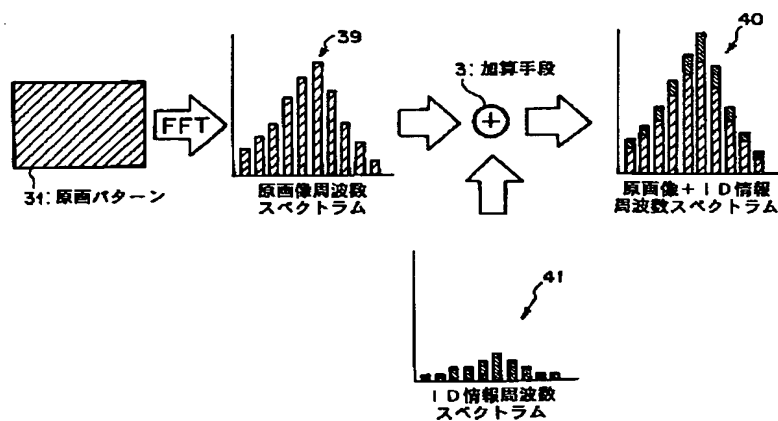
【図 9】



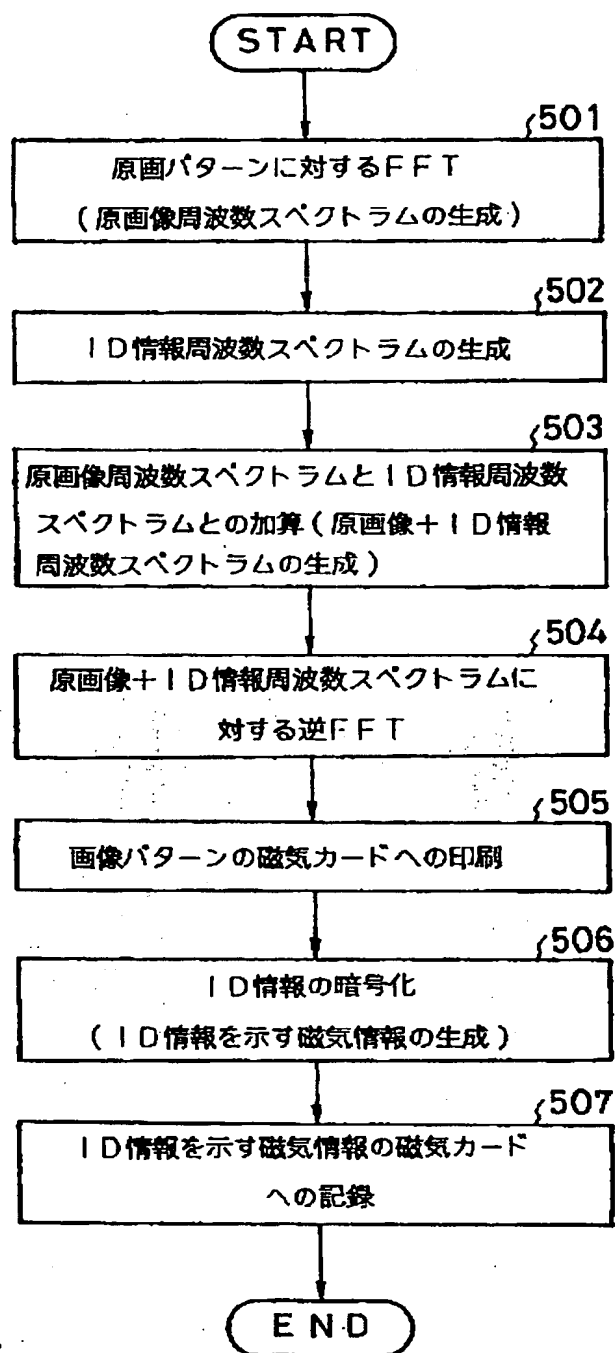
【図 7】



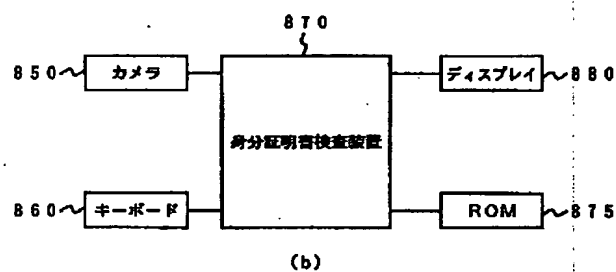
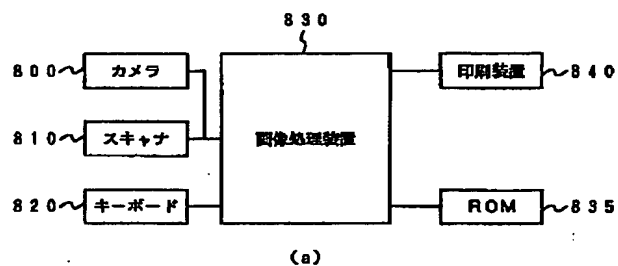
【図 8】



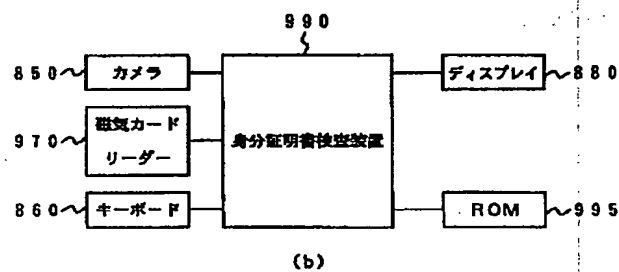
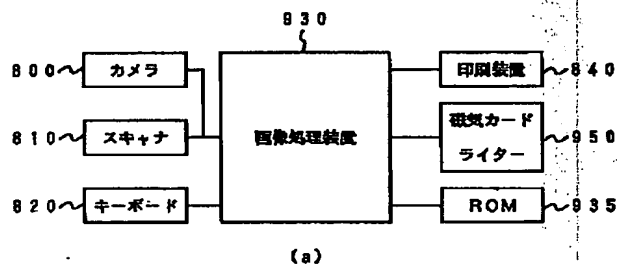
【図11】



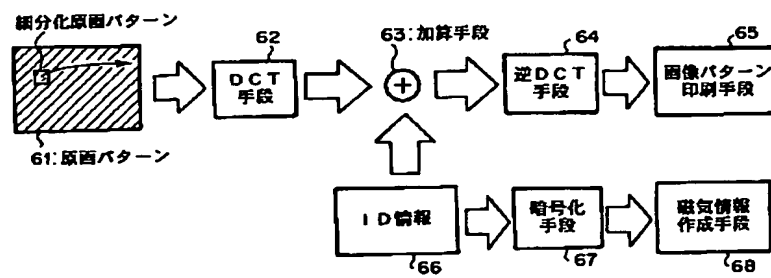
【図16】



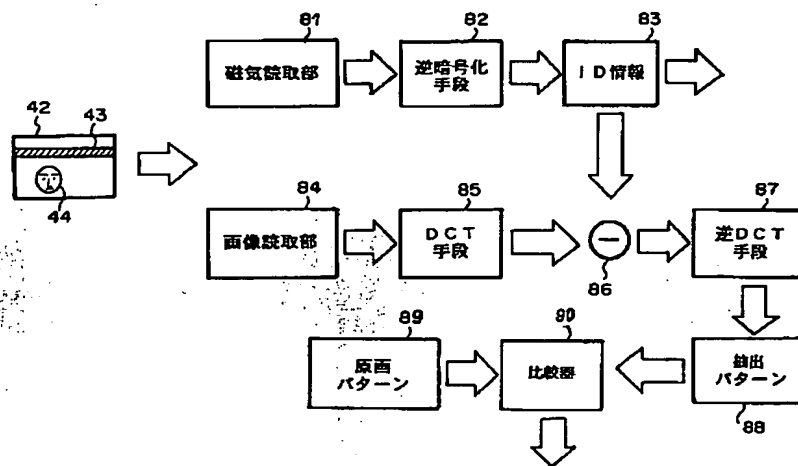
【図19】



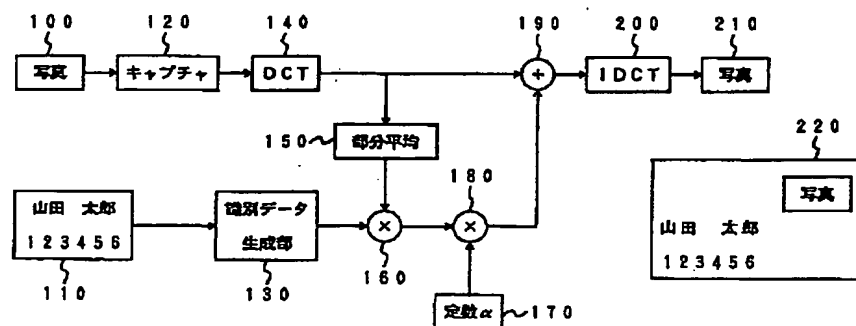
【図12】



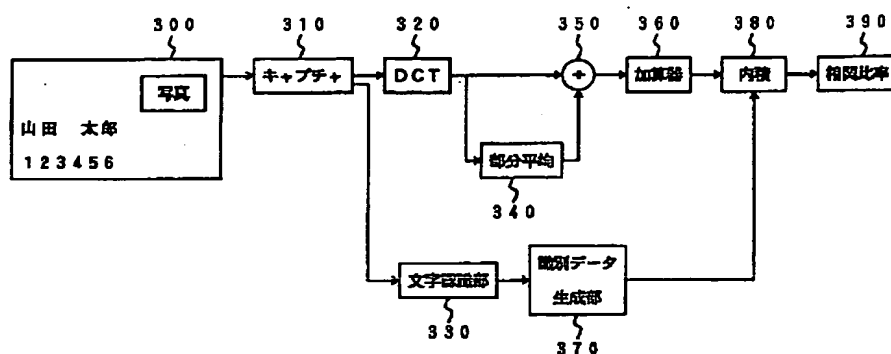
【図13】



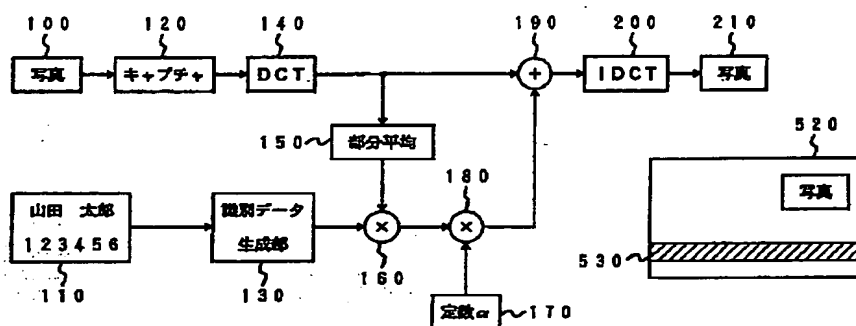
【図14】



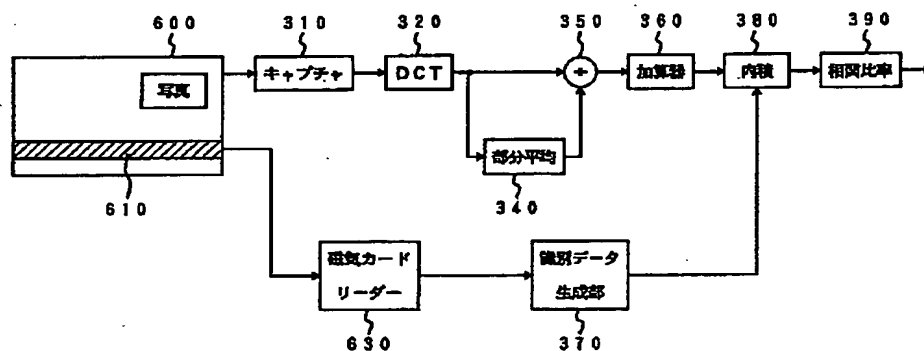
【図15】



【図17】



【図18】



フロントページの続き

(51) Int. Cl.⁶

H04L 9/32

識別記号

F I

H04L 9/00

673C

673A

673E